Bitdefender®

INTERNET SECURITY 2015



BENUTZERHANDBUCH

Bitdefender Internet Security 2015
Benutzerhandbuch

Veröffentlicht 20.10.2014

Rechtlicher Hinweis



Inhaltsverzeichnis

INSTALLATION

1. VOR DER INSTALLATION

Bevor Sie Bitdefender Internet Security 2015 installieren, sollten Sie für eine reibungslose Installation sicherstellen, dass folgende Schritte durchgeführt wurden:

- Stellen Sie sicher, dass der Zielcomputer für die Bitdefender-Installation die Systemvoraussetzungen erfüllt. Wenn Ihr Computer nicht die Mindest-Systemanforderungen erfüllt, kann Bitdefender nicht installieren werden. Wird die Systemkonfiguration nachträglich verändert, kann es zu Leistungseinbußen und Stabilitätsproblemen kommen. Eine vollständige Liste der Systemanforderungen finden Sie unter *„Systemanforderungen“* (S. 3).
- Melden Sie sich mit einem Administrator-Konto am Computer an.
- Entfernen Sie alle anderen Sicherheitslösungen von Ihrem Computer. Die gleichzeitige Nutzung mehreren Sicherheitsprogrammen kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen. Windows Defender wird während der Installation deaktiviert.
- Deaktivieren oder entfernen Sie jegliche Firewall-Programme, die auf dem PC installiert sind. Die gleichzeitige Nutzung mehreren Sicherheitsprogrammen kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen. Die Windows-Firewall wird während der Installation deaktiviert.
- Ihr Computer sollte während der Installation mit dem Internet verbunden sein, selbst wenn Sie von CD oder DVD installieren. Falls neuere Versionen der Anwendungsdateien aus dem Installationspaket verfügbar sind, kann Bitdefender diese dann herunterladen und installieren.

2. SYSTEMANFORDERUNGEN

Sie können Bitdefender Internet Security 2015 nur auf Computern mit den folgenden Betriebssystemen installieren.

- Windows XP mit Service Pack 3 (32-Bit)
- Windows Vista mit Service Pack 2
- Windows 7 mit Service Pack 1
- Windows 8
- Windows 8.1

Stellen Sie vor der Installation sicher, dass Ihr Computer die Mindestsystemanforderungen erfüllt.



Beachten Sie

Für Informationen zu Ihrem Windows-Betriebssystem und Ihrer Hardware gehen Sie folgendermaßen vor:

- Rechtsklicken Sie in **Windows XP**, **Windows Vista** und **Windows 7** auf Ihrem Desktop auf **Arbeitsplatz** und wählen Sie danach den Menüpunkt **Eigenschaften**.
- In **Windows 8**, finden Sie auf der Windows-Startseite den Eintrag Computer(z.B. durch die Eingabe von "Computer" auf der Startseite) und klicken Sie auf das entsprechende Symbol. Wählen Sie im Menü unten Eigenschaften. Unter System finden Sie Ihren Systemtyp.

2.1. Mindestsystemanforderungen

- 1 GB freier Speicherplatz (davon mindestens 800 MB auf dem Systemlaufwerk)
- 1.6-GHz-Prozessor
- 1 GB Arbeitsspeicher (RAM) für Windows XP, Windows Vista, Windows 7 und Windows 8

2.2. Empfohlene Systemanforderungen

- 2 GB freier Speicherplatz (davon mindestens 800 MB auf dem Systemlaufwerk)
- Intel CORE 2 Duo (2 GHz) oder gleichwertiger Prozessor
- Speicher (RAM):
  - 1 GB MB für Windows XP

- 1,5 GB für Windows Vista, Windows 7 und Windows 8

2.3. Software-Anforderungen

Um Bitdefender und alle Funktionen nutzen zu können, muss Ihr Computer die folgenden Software-Anforderungen erfüllen:

- Internet Explorer 8 oder höher
- Mozilla Firefox 14 oder höher
- Chrome 20 oder höher
- Skype 6.3 oder höher
- Yahoo! Messenger 9 oder höher
- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express und Windows Mail (auf 32-Bit-Systemen)
- Mozilla Thunderbird 14 oder höher
- .NET Framework 3.5 (wird, wenn nicht vorhanden, automatisch mit Bitdefender mit installiert)

3. INSTALLIEREN IHRES BITDEFENDER-PRODUKTS

Sie können Bitdefender von der Bitdefender-Installations-CD oder über ein Installationspaket installieren, das Sie von der Bitdefender- Website oder einer anderen autorisierten Website heruntergeladen haben (so z.B. von einer Bitdefender-Partner-Website oder einem Online-Shop). Sie können das Installationspaket von der Bitdefender Webseite unter folgender Adresse herunterladen: http://www.bitdefender.de/Downloads/.

Wenn Sie eine Lizenz für mehr als einen Computer haben, (wenn Sie z. B. Bitdefender Internet Security 2015 für 3 PCs gekauft haben), wiederholen Sie den Installationsvorgang und die Registrierung mit dem Lizenzschlüssel auf jedem Computer.

- Um Bitdefender von der Installations-CD aus zu installieren, legen Sie die CD in das optische Laufwerk ein. Ein Willkommens-Bildschirm sollte nach wenigen Augenblicken angezeigt werden. Folgen Sie den Anweisungen, um die Installation zu starten.



Beachten Sie

Im Willkommensbildschirm haben Sie die Möglichkeit, das Installationspaket von der Installations-CD auf einen USB-Speicherstick zu kopieren. Dies kann sich als nützlich erweisen, wenn Sie Bitdefender auf einem Computer installieren wollen, der über kein Laufwerk verfügt (wie z.B. ein Netbook). Verbinden Sie das Speichermedium mit einem USB Port und klicken Sie auf **Kopiere auf USB**. Stecken Sie den Speicherstick anschließend in den USB-Port des Computers ohne Laufwerk und doppelklicken Sie in dem Ordner, in dem Sie das Installationspaket gespeichert haben, auf runsetup.exe.

Wenn der Willkommensbildschirm nicht angezeigt wird, öffnen Sie im Windows-Explorer das Root-Verzeichnis der CD und doppelklicken Sie auf autorun.exe.

- Um Bitdefender über das von Ihnen heruntergeladene Installationspaket zu installieren, navigieren Sie zu der Datei und doppelklicken Sie darauf.

Validierung der Installation

Bitdefender wird zuallererst Ihr System überprüfen, um die Installation zu bestätigen.

Wenn Ihr System die Mindestanforderungen zur Installation von Bitdefender nicht erfüllt, werden Sie darüber informiert, welche Bereiche aufgerüstet werden müssen, damit Sie fortfahren können.

Wenn ein inkompatibles Virenschutzprogramm oder eine ältere Version von Bitdefender erkannt wird, werden Sie aufgefordert, diese von Ihrem System zu entfernen. Bitte folgen Sie den Anweisungen, um die Software von Ihrem System zu entfernen und so spätere Probleme zu vermeiden. Unter Umständen müssen Sie Ihren Computer neu starten, um die Entfernung der erkannten Virenschutzprogramme abzuschließen.

Das Installationspaket für Bitdefender Internet Security 2015 wird ständig aktualisiert. Wenn Sie die Software von einer CD/DVD installieren, kann Bitdefender die aktuelle Version der Dateien während der Installation herunterladen. Klicken Sie dazu auf **Ja**, wenn Sie dazu aufgefordert werden. Bitdefender lädt dann die Dateien herunter und gewährleistet so, dass Sie die aktuelle Version der Software installieren.



Beachten Sie

Das Herunterladen der Installationsdateien kann eine Weile dauern, besonders bei langsameren Internetverbindungen.

Sobald die Installation validiert ist, startet der Installationsassistent. Folgen Sie den Schritten, um Bitdefender Internet Security 2015 auf Ihrem PC zu installieren.

Schritt 1 - Willkommen

Im Willkommensbildschirm können Sie entscheiden, welche Art von Installation Sie wünschen.

Wenn Sie sich nicht um Detaileinstellungen kümmern möchten, klicken Sie einfach auf **Installieren**. Bitdefender wird dann mit den Standardeinstellungen im Standardpfad installiert, und Sie können direkt mit Schritt 3 das Assistenten fortfahren.

Klicken Sie zur Konfiguration der Installationseinstellungen auf **Benutzerdef.**.

In diesem Schritt können Sie zwei zusätzliche Dinge tun:

- Bitte lesen Sie vor der Installation die Endbenutzer-Lizenzvereinbarung. Die Lizenzvereinbarung enthält die Nutzungsbedingungen für Bitdefender Internet Security 2015.

Sollten Sie diesen Nutzungsbedingungen nicht zustimmen, schließen Sie das Fenster. Der Installationsprozess wird abgebrochen uns Sie verlassen den Assistenten.

- Senden von **anonymen Nutzungsberichten** aktivieren. Durch Aktivierung dieser Option, werden Berichte, die Informationen zu Ihrer Nutzung des Produktes an Bitdefender Server gesendet. Diese Information ist wichtig für die Verbesserung des Produktes. Bitte beachten Sie, dass diese Berichte weder vertrauliche Daten, wie Ihren Namen und Ihre IP Adresse, enthalten, noch werden diese Daten für kommerzielle Zwecke verwendet.

Schritt 2 - Installation individuell anpassen



Beachten Sie

Dieser Schritt kommt nur dann vor, wenn Sie die benutzerdefinierte Installation gewählt haben.

Die folgenden Optionen sind verfügbar:

Installationspfad

Bitdefender Internet Security 2015 wird standardmäßig im Ordner C:\Programme\Bitdefender\Bitdefender Internet Security 2015 installiert. Falls Sie ein anderes Installationsverzeichnis wählen möchten, klicken Sie auf **Ändern** und wählen Sie das Verzeichnis, in dem Sie Bitdefender installieren möchten.

Proxy-Einstellgn. konf.

Bitdefender Internet Security 2015 benötigt Zugriff auf das Internet, um die Produktregistrierung abzuschließen, Sicherheits- und Produkt-Updates herunterzuladen, In-the-Cloud-Komponenten zu nutzen usw. Wenn Sie eine Proxy-Verbindung anstelle einer direkten Internet-Verbindung nutzen, müssen Sie diese Option auswählen und die Proxy-Einstellungen konfigurieren.

Die Einstellungen können aus dem Standard-Browser importiert oder manuell eingegeben werden.

Klicken Sie auf **Installieren**, um Ihre Einstellungen zu bestätigen und mit der Installation zu beginnen. Wenn Sie sich später umentscheiden, können Sie einfach auf die entsprechende **Standard verwenden**-Schaltfläche klicken.

Schritt 3 - Installation wird durchgeführt

Bitte warten Sie, bis der Installationsvorgang abgeschlossen ist. Sie erhalten detaillierte Informationen über den Fortschritt der Installation.

Kritische Bereiche Ihres Systems werden nach Viren durchsucht, die neuesten Versionen der Anwendungsdateien heruntergeladen und installiert und die Bitdefender-Dienste gestartet. Dieser Schritt kann einige Minuten in Anspruch nehmen.

Schritt 4 - Installation ist abgeschlossen

Eine Zusammenfassung der Installation wird angezeigt. Sollte während der Installation aktive Malware erkannt und entfernt werden, könnte ein Neustart des Systems erforderlich werden.

Sie können entweder das Fenster schließen oder mit einem Klick auf **Erste Schritte** mit der Ersteinrichtung der Software beginnen.

Schritt 5 - Produkt registrieren



Beachten Sie

Dieser Schritt erfolgt nur, wenn Sie im vorigen Schritt "Erste Schritte" gewählt haben.

Um Ihr Produkt zu registrieren, müssen Sie einen Lizenzschlüssel eingeben. Zudem wird eine aktive Internet-Verbindung benötigt.

Gehen Sie abhängig von Ihrer persönlichen Situation folgendermaßen vor:

- **Ich habe das Produkt erworben**

  In diesem Fall registrieren Sie das Produkt, indem Sie die folgenden Schritte ausführen:

  1. Wählen Sie den Punkt **Ich habe Bitdefender erworben und möchte es jetzt registrieren**.
  2. Geben Sie den Lizenzschlüssel in das entsprechende Feld ein.

  ### Beachten Sie

  Sie finden den Lizenzschlüssel:
  - auf dem Label der CD/DVD.
  - auf dem Lizenzzertifikat.

- In der E-Mail-Bestätigung des Online-Kaufs.

3. Klicken Sie auf **Jetzt registrieren**.

- **Ich habe keinen Lizenzschlüssel, ich möchte das Produkt kostenlos testen**

  In diesem Fall können Sie das Produkt für 30 Tage nutzen. Um die Testphase zu starten, klicken Sie auf **Ich habe keinen Lizenzschlüssel, ich möchte das Produkt kostenlos testen**.

- Klicken Sie auf **Weiter**.

Schritt 6 - Produktverhalten konfigurieren

Bitdefender kann so konfiguriert werden, dass es die Programme automatisch erkennt, die Sie für Ihre Arbeit benötigen, und Ihnen so das Arbeiten in bestimmten Situationen erleichtern. Über den Schalter können Sie **Profile** aktivieren oder deaktivieren.

Aktivieren Sie Ihre **Profile**, wenn Sie arbeiten, spielen oder Filme schauen. Dadurch werden die Produkt- und Systemeinstellungen so angepasst, dass die Auswirkungen auf die Systemleistung minimiert werden. Für weitere Informationen lesen Sie bitte *„Profile“* (S. 19).

Klicken Sie auf **Weiter**.

Schritt 7 - Produkt aktivieren

Sie benötigen ein MyBitdefender-Konto, um die Online-Funktionen der Software zu nutzen. Für weitere Informationen lesen Sie bitte *„MyBitdefender-Konto“* (S. 42).

Fahren Sie entsprechend Ihrer Situation fort.

Ich möchte ein MyBitdefender-Konto anlegen

Um ein MyBitdefender-Konto erfolgreich anzulegen, gehen Sie folgendermaßen vor:

1. Wählen Sie **Benutzerkonto anlegen**.

   Ein neues Fenster wird sich öffnen.

2. Geben Sie die Daten in die entsprechenden Felder ein. Die hier eingetragenen Daten bleiben vertraulich.

   - **E-mail** - Geben Sie Ihre E-Mail-Adresse an.

- **Benutzername** - Geben Sie einen Benutzernamen für Ihr Konto ein.
- **Passwort** - Geben Sie ein Passwort für Ihr Benutzerkonto ein. Das Passwort muss mindestens 6 Zeichen lang sein.
- **Passwort bestätigen** - Geben Sie das Passwort erneut ein.



Beachten Sie
Sobald das Benutzerkonto angelegt wurde, können Sie sich mit der angegebenen E-Mail-Adresse und dem Passwort unter https://my.bitdefender.com bei Ihrem Konto anmelden.

3. Klicken Sie auf **Erstellen**.
4. Bevor Sie Ihr Konto nutzen können, müssen Sie zunächst die Registrierung abschließen. Rufen Sie Ihre E-Mails ab und folgen Sie den Anweisungen in der Bestätigungsnachricht, die Sie von Bitdefender erhalten haben.

Ich möchte mich über mein Microsoft-, Facebook- oder Google-Konto anmelden

Um sich über Ihr Microsoft-, Facebook- oder Google-Konto anzumelden, gehen Sie folgendermaßen vor:

1. Wählen Sie, worüber Sie sich anmelden möchten. Sie werden auf die Anmeldeseite dieses Dienstes weitergeleitet.
2. Folgen Sie den Anweisungen des ausgewählten Dienstes, um Ihr Benutzerkonto mit Bitdefender zu verknüpfen.



Beachten Sie
Bitdefender hat keinen Zugriff auf Ihre vertraulichen Informationen, so zum Beispiel das Passwort, das Sie zur Anmeldung an Ihrem Konto verwenden, oder die persönlichen Informationen Ihrer Freunde und Kontakte.

Ich habe bereits ein MyBitdefender-Konto

Wenn Sie sich von Ihrem Produkt aus bereits zuvor bei einem Benutzerkonto angemeldet haben, wird Bitdefender dies erkennen und Sie auffordern, das Passwort einzugeben, um sich bei diesem Benutzerkonto anzumelden.

Wenn Sie bereits ein aktives Konto haben, Bitdefender es aber nicht erkennt, oder wenn Sie sich bei einem anderen Konto anmelden möchten,

geben Sie die E-Mail-Adresse und das Passwort ein, und klicken Sie anschließend auf **Bei MyBitdefender anmelden**.

Erst einmal aufschieben

Wenn Sie sich später um diesen Punkt kann man möchten, klicken Sie auf **Später nachfragen**. Beachten Sie dabei, dass Sie sich bei einem Konto anmelden müssen, um die Online-Funktionen des Produkts zu nutzen.

INBETRIEBNAHME

4. GRUNDLAGEN

Sobald Sie Bitdefender Internet Security 2015 installiert haben, ist Ihr Computer gegen jede Art von Malware (wie beispielsweise Viren, Spyware und Trojaner) und andere Internetbedrohungen (wie Hacker, Phishing und Spam) geschützt.

Die Anwendung nutzt die Photon-Technologie, um Malware-Scans zu beschleunigen und noch leistungsfähiger zu machen. Diese lernt, wie Sie die Anwendungen auf Ihrem System nutzen, und weiß so, was sie wann scannen soll. Dadurch werden die Auswirkungen auf die Systemleistung minimiert.

Sie können den Autopilot einschalten und beruhigt Sicherheit im Hintergrund genießen, ohne dass sie selbst irgendwelche Einstellungen vornehmen müssen. Sie können jedoch auch die Bitdefender-Einstellungen für die Feineinstellung nutzen und Ihren Schutz verbessern.

Bitdefender ermöglicht Ihnen ein störungsfreies Arbeiten, Spielen und Abspielen von Filmen, indem es Wartungsaufgaben aufschiebt, Unterbrechungen verhindert und die visuellen Einstellungen entsprechend anpasst. Sie können von all dem profitieren, indem Sie Ihre Profile aktivieren oder konfigurieren.

Bitdefender trifft alle sicherheitsrelevanten Entscheidungen für Sie und wird nur in seltenen Fällen Pop-up-Benachrichtigungen anzeigen. Nähere Informationen zu den durchgeführten Aktionen und zur Programmausführung finden Sie im Ereignisfenster. Für weitere Informationen lesen Sie bitte *„Ereignisanzeige“* (S. 16).

Von Zeit zu Zeit sollten Sie Bitdefender öffnen und existierende Probleme beheben. Es ist möglich, dass-Sie, um Ihren Computer und Ihre Daten zu schützen, bestimmte Bitdefender-Komponenten konfigurieren oder vorbeugende Maßnahmen durchführen müssen.

Wenn Sie das Produkt noch nicht registriert haben, sollten Sie dies vor Ablauf der Testphase noch tun. Für weitere Informationen lesen Sie bitte *„Bitdefender registrieren“* (S. 40).

Um die Online-Funktionen von Bitdefender Internet Security 2015 zu nutzen, muss Ihr Computer mit einem MyBitdefender-Konto verknüpft sein. Für weitere Informationen lesen Sie bitte *„MyBitdefender-Konto“* (S. 42).

Im Abschnitt „Gewusst wie“ (S. 49) finden Sie detaillierte Anweisungen zur Ausführung der häufigsten Aufgaben. Wenn Sie bei der Verwendung von Bitdefender Probleme haben, finden Sie im Abschnitt *„Verbreitete Probleme beheben“* (S. 199) Lösungen zu den häufigsten Problemen.

4.1. Das Bitdefender-Fenster öffnen

Um das Bitdefender Internet Security 2015-Hauptfenster aufzurufen, gehen Sie folgendermaßen vor:

- Für **Windows XP**, **Windows Vista** und **Windows 7**:
  1. Klicken Sie auf **Start** und **Alle Programme**.
  2. Klicken Sie auf **Bitdefender 2015**.
  3. Klicken Sie auf **Bitdefender Internet Security 2015**. Noch schneller geht es mit einem Doppelklick auf das Bitdefender-Symbol B in der Task-Leiste.
- In **Windows 8**:

  Finden Sie auf der Windows-Startseite Bitdefender Internet Security 2015 (z.B. durch die Eingabe von "Bitdefender" auf der Startseite) und klicken Sie auf das entsprechende Symbol. Öffnen Sie alternativ die Desktop-App und doppelklicken Sie danach auf das Bitdefender B-Symbol in der Task-Leiste.

Weitere Informationen zum Bitdefender-Fenster und das Symbol in der Task-Leiste finden Sie im Kapitel *„Bitdefender-Benutzeroberfläche“* (S. 25).

4.2. Probleme beheben

Bitdefender benutzt ein Problem-Tracking-System, um sicherheitsgefährdende Probleme festzustellen und Sie über diese zu informieren. Standardmässig wird nur ein Teil der für am wichtigsten erachteten Risiken überwacht. Sie können dies nach Bedarf verändern, wählen Sie aus über welche Risiken sie informiert werden möchten.

Zu den gefundenen Problemen gehören auch wichtige Schutzeinstellungen, die deaktiviert sind, und andere Umstände, die ein Sicherheitsrisiko darstellen. Sue sind in zwei Kategorien unterteilt:

- **Kritische Probleme** - Verhindern, dass Bitdefender Sie vor Malware schützt oder stellen ein erhebliches Sicherheitsrisiko dar.

- **Kleinere (nicht-kritische) Probleme** - Können Ihren Schutz in naher Zukunft beeinträchtigen.

Das Bitdefender-Symbol in der Task-Leiste weist Sie durch die folgenden Farbwechsel auf ausstehende Probleme hin:

Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.
Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.

Wenn Sie den Mauszeiger über das Symbol bewegen, wird Ihnen angezeigt, dass ein Problem existiert.

Wenn Sie das Bitdefender-Fenster öffnen, zeigt der Sicherheitsstatusbereich in der oberen Symbolleiste die Art der Probleme an, die Ihr System beeinträchtigen.

4.2.1. "Alle Probleme beheben"-Assistent

Um erkannte Probleme zu beheben, folgen Sie den Anweisungen des **Alle Probleme beheben**-Assistenten.

1. Befolgen Sie eine der folgenden Möglichkeiten, den Assistenten zu öffnen:
   - Rechtsklicken Sie auf das Bitdefender-Symbol in der Task-Leiste und wählen Sie dann **Sicherheitsprobleme anzeigen**.
   - Öffnen Sie das Bitdefender-Fenster und klicken Sie auf eine beliebige Stelle innerhalb des Sicherheitsstatusbereichs in der oberen Symbolleiste (Sie können zum Beispiel auf die Schaltfläche**Alle Probleme beheben!** klicken).
2. Sie erhalten eine Übersicht aller Probleme, die die Sicherheit Ihres Computers und Ihrer Daten beeinträchtigen. Alle aktuellen Probleme sind markiert und werden behoben.

   Wenn Sie ein bestimmtes Problem nicht sofort beheben möchten, deaktivieren Sie das entsprechende Kästchen. Sie werden aufgefordert anzugeben, für wie lange die Behebung des Problems verschoben werden soll. Wählen Sie die gewünschte Option aus dem Menü und klicken Sie auf **OK**. Um die Überwachung der jeweiligen Problemkategorie zu beenden, wählen Sie den Punkt **Dauerhaft**.

Der Status des Problems erscheint als **Aufschieben** und es wird keine Aktion zur Behebung des Problems durchgeführt.

3. Um die ausgewählten Probleme zu beheben, klicken Sie auf **Beheben**. Manche Probleme werden sofort behoben. Bei anderen hilft Ihnen ein Assistent bei der Behebung.

Die Risiken die Ihnen dieser Assistent hilft zu beheben, können in diese Hauptkategorien eingeordnet werden

- **Deaktivierte Sicherheitseinstellungen.** Solche Probleme werden sofort beseitigt, durch die entsprechenden Sicherheitseinstellungen.
- **Vorbeugende Sicherheitsaufgaben die Sie durchführen sollten.** Bei der beseitigung solcher Probleme, hilft Ihnen ein Assistent.

4.2.2. Konfigurieren von Statusbenachrichtigungen

Bitdefender kann Sie informieren, wenn in einer der folgenden Komponenten ein Problem aufgetreten ist:

- Firewall
- Antispam
- Antivirus
- Update
- Browser-Sicherheit

Sie können das Warnsystem ganz nach Ihren individuellen Ansprüchen konfigurieren, indem Sie wählen, über welche Ereignisse Sie informiert werden möchten. Folgen Sie diesen Schritten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Erweitert** aus.
4. Klicken Sie auf **Statusbenachrichtigungen konfigurieren**.
5. Klicken Sie auf die Schalter, um die Statusbenachrichtigungen entsprechend Ihrer Anforderungen zu aktivieren oder deaktivieren.

4.3. Ereignisanzeige

Bitdefender führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer. Immer wenn etwas passiert, was die Sicherheit

Ihres Systems oder ihrer Daten betrifft, wird in den Bitdefender-Ereignissen eine Nachricht erstellt, ähnlich einer neuen E-Mail in Ihrem Postfach.

Ereignisse sind ein wichtiges Hilfsmittel für die Überwachung und Verwaltung Ihres Bitdefender-Schutzes. So können Sie beispielsweise einfach überprüfen ob das Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem entdeckt wurde usw. Zudem können Sie bei Bedarf weitere Aktionen ausführen oder die von Bitdefender ausgeführten Aktionen anpassen.

So öffnen Sie das Ereignisprotokoll:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.

Die Nachrichten werden nach dem Bitdefender-Modul sortiert, zu dem sie gehören:

- **Antivirus**
- **Firewall**
- **Angriffserkennung**
- **Internet-Schutz**
- **Antispam**
- **Safego**
- **PC-Tuning**
- **Schwachstelle**
- **Update**

Bei jedem Ereignis wird im -Symbol oben im Fenster ein blauer Punkt angezeigt.

Eine Liste von Ereignissen ist für jede Kategorie verfügbar. Um Informationen über ein bestimmtes Ereignis in der Liste abzurufen, klicken Sie auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus. Details zu dem Ereignis werden in der unteren Hälfte des Fensters angezeigt. Sie erhalten die folgenden Informationen zu jedem Ereignis: eine Kurzbeschreibung; die Aktion, die Bitdefender für beim Auftreten des Ereignisses durchgeführt hat; das Datum und der Zeitpunkt des Ereignisses. Unter Umständen werden Ihnen Optionen zur weiteren Vorgehensweise angeboten.

Sie können Ereignisse nach Wichtigkeit und nach Reihenfolge ihres Auftretens sortieren. Es gibt drei Arten von Ereignissen, die nach ihrer Wichtigkeit sortiert werden. Diese werden durch verschiedene Symbole unterschieden:

■ **Information** Diese Ereignisse weisen auf erfolgreich ausgeführte Vorgänge hin.
■ **Warnung** Diese Ereignisse weisen auf nicht-kritische Probleme hin. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
■ **Kritische** Ereignisse weisen auf kritische Probleme hin. Sie sollten sich umgehend darum kümmern.

Um alle Ereignisse anzuzeigen, die über einem bestimmten Zeitraum aufgetreten sind, wählen Sie den gewünschten Zeitraum im entsprechenden Feld aus.

Um Ihnen die Verwaltung von protokollierten Ereignissen zu erleichtern, enthält jeder Abschnitt des Ereignisfensters Optionen, mit denen Sie alle Ereignisse in diesem Abschnitt löschen oder als gelesen markieren können.

4.4. Autopilot

Für alle Benutzer, die nichts weiter von Ihrer Sicherheitslösung erwarten, als zuverlässigen Schutz, ohne bei der Arbeit gestört zu werden, bietet Bitdefender Internet Security 2015 einen integrierten Autopilot-Modus.

Solange der Autopilot aktiviert ist, wird Bitdefender die optimale Sicherheitskonfiguration anwenden und alle sicherheitsrelevanten Entscheidungen für Sie treffen. Das bedeutet, dass keine Pop-ups oder Benachrichtigungen eingeblendet werden und Sie keinerlei Einstellungen vornehmen müssen.

Wenn der AutoPilot aktiviert ist, werden kritische Probleme von Bitdefender automatisch behoben. Zudem werden die folgenden Funktionen unauffällig im Hintergrund verwaltet:

- Virenschutz, gewährleistet durch Zugriff-Scans und ununterbrochenes Scanning.
- Firewall-Schutz.
- Internet-Schutz.
- Automatische Updates.

So schalten Sie den Autopiloten ein und aus:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie auf den Schalter **Humanmodus/Autopilot** in der oberen Symbolleiste.. Wenn der Schalter auf Humanmodus steht, ist der Autopilot ausgeschaltet.

Wenn der Autopilot eingeschaltet ist, erscheint folgendes Bitdefender-Symbol in der Task-Leiste: .



Wichtig

Wenn der Autopilot eingeschaltet ist und Sie eine der von ihm verwalteten Einstellungen verändern, wird er automatisch ausgeschaltet.

Um eine Übersicht der Aktionen anzuzeigen, die von Bitdefender durchgeführt wurden, während der Autopilot eingeschaltet war, öffnen Sie das Fenster Ereignisse.

4.5. Profile und Akkubetrieb

Bei einigen Aktivitäten am Computer, so zum Beispiel bei Online-Spielen oder Videopräsentationen, werden schnelle Reaktionszeiten und konstant hohe Systemleistung ohne Unterbrechungen benötigt. Wenn Ihr Laptop auf Batteriebetrieb läuft ist es ratsamer unnötige Vorgänge, welche zusätzlich Strom verbrauchen, zu verschieben, bis der Laptop extern mit Strom versorgt wird.

Um sich diesen besonderen Situationen anzupassen, hat Bitdefender Internet Security 2015 zwei spezielle Betriebsmodi:

- Profile
- Akkubetrieb

4.5.1. Profile

Bitdefender-Profile weist den laufenden Anwendungen zusätzliche Systemressourcen zu, indem er die Schutzeinstellungen vorübergehend modifiziert und die Systemkonfiguration entsprechend anpasst. So werden die Systemauswirkungen auf Ihre jeweilige Aktivität minimiert.

Um den verschiedenen Aktivitäten gerecht zu werden, enthält Bitdefender die folgenden Profile:

Arbeitsprofil
Sorgt für optimale Arbeitseffizienz, indem es die Produkt- und Systemeinstellungen erkennt und entsprechend anpasst.

Filmprofil
Verbessert die visuellen Effekte und sorgt für störungsfreies Filmvergnügen.

Spielprofil
Verbessert die visuellen Effekte und sorgt für störungsfreies Spielvergnügen.

Aktivieren und Deaktivieren von Profilen

So können Sie die Profile aktivieren oder deaktivieren:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Wählen Sie im Fenster **Profile** den Reiter **Profileinstellungen** aus.
5. Aktivieren oder deaktivieren Sie die Profile, indem Sie auf den entsprechenden Schalter klicken.

Autopilot zur Überwachung der Profile konfigurieren

Für noch mehr Benutzerfreundlichkeit können Sie den Autopilot so konfigurieren, dass er Ihr Arbeitsprofil verwaltet. In diesem Modus erkennt Bitdefender automatisch Ihre jeweiligen Aktivitäten und optimiert den System- und Produktbetrieb entsprechend.

So konfigurieren Sie den Autopilot zur Verwaltung Ihrer Profile:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Wählen Sie im Fenster **Profile** den Reiter **Profileinstellungen** aus.
5. Klicken Sie auf den entsprechenden **Autopilot soll meine Profile verwalten**-Schalter.

Wenn Sie nicht möchten, dass Ihr Profil automatisch verwaltet werden, aktivieren Sie das Kästchen nicht und wählen Sie es manuell oben rechts aus der Bitdefender-Benutzeroberfläche aus.

Weitere Informationen zur Profile finden Sie im Kapitel *„Profile“* (S. 192)

4.5.2. Akkubetrieb

Der Akkubetrieb wurde speziell für Laptop- und Tablet-Nutzer entwickelt. Er minimiert die Auswirkungen des System- und Bitdefender-Betriebs auf die Akkulaufzeit, sobald der von Ihnen festgelegte Akkuladestand unterschritten wird.

Die folgenden Produkteinstellungen werden angewendet, wenn Bitdefender in den Akkubetrieb versetzt wird:

- Automatische Bitdefender-Updates werden verschoben.
- Geplante Scans werden verschoben.
- Das Sicherheits-Widget wird deaktiviert.

Bitdefender erkennt, wenn Ihr Laptop vom Stromnetz getrennt wird und startet den Akkubetrieb automatisch je nach festgelegten Akkuladestand. Ebenso beendet Bitdefender automatisch den Akkubetrieb, wenn der Laptop nicht mehr über den Akku betrieben wird.

So können Sie den Akkubetrieb aktivieren oder deaktivieren:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Wählen Sie im Fenster **Profile** den Reiter **Akkubetrieb** aus.
5. Aktivieren oder deaktivieren Sie den automatischen Akkubetrieb, indem Sie auf den entsprechenden Schalter klicken.

   Schieben Sie den entsprechenden Regler auf den Wert, bei dem das System in den Akkubetrieb wechseln soll. Standardmäßig wird der Akkubetrieb aktiviert, sobald der Akkuladestand unter 30 % sinkt.



Beachten Sie

Der Akkubetrieb ist auf Laptops und Tablets standardmäßig aktiviert.

Konfigurieren des Akkubetriebs

So konfigurieren Sie den Akkubetrieb:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Wählen Sie im Fenster **Profile** den Reiter **Akkubetrieb** aus.
5. Klicken Sie auf **Konfigurieren**.
6. Wählen Sie die durchzuführenden Systemanpassungen aus, indem Sie die folgenden Optionen auswählen:
   - Produkteinstellungen für den Akkubetrieb optimieren.
   - Hintergrundprogramme und Wartungsaufgaben verschieben.
   - Automatische Windows-Updates später durchführen.
   - Energiesparplaneinstellungen für den Akkubetrieb anpassen.
   - Externe Geräte und Netzwerk-Ports deaktivieren.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

4.6. Passwortschutz für Bitdefender-Einstellungen

Wenn Sie nicht der einzige Benutzer des Computers sind, empfehlen wir Ihnen, Ihre vorgenommenen Einstellungen mit einem Passwort zu schützen.

Um den Passwortschutz für die Bitdefender-Einstellungen zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Allgemeine Einstellungen** aus.
4. Aktivieren Sie den Passwortschutz, indem Sie auf den Schalter klicken.
5. Geben Sie das Passwort in die beiden Felder ein und klicken Sie dann auf **OK**. Das Passwort muss mindestens 8 Zeichen lang sein.

Sobald Sie ein Passwort festgelegt haben, muss jeder, der die Bitdefender-Einstellungen verändern will, zunächst das Passwort eingeben.



Wichtig

Merken Sie sich Ihr Passwort gut oder schreiben Sie es auf und verwahren es an einem sicheren Platz. Wenn Sie Ihr Passwort vergessen haben, müssen Sie das Programm neu installieren oder den Kundendienst von Bitdefender kontaktieren.

Um den Passwortschutz zu deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Allgemeine Einstellungen** aus.
4. Deaktivieren Sie den Passwortschutz, indem Sie auf den Schalter klicken. Geben Sie das Passwort ein und klicken Sie auf **OK**.



Beachten Sie

Um das Passwort für Ihr Produkt zu ändern, klicken Sie auf **Passwort ändern**.

4.7. Anonyme Nutzungsberichte

Bitdefender verschickt standardmäßig Berichte mit Nutzungsinformationen an die Bitdefender-Server. Diese Information ist wichtig für die Verbesserung des Produktes. Bitte beachten Sie, dass diese Berichte weder vertrauliche Daten, wie Ihren Namen und Ihre IP Adresse, enthalten, noch werden diese Daten für kommerzielle Zwecke verwendet.

Wenn Sie das Versenden von anonymen Nutzungsberichten beenden wollen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Erweitert** aus.
4. Klicken Sie auf den Schalter, um anonyme Nutzungsberichte auszuschalten.

4.8. Sonderangebote und Produktbenachrichtigungen

Sind Sonderangebote verfügbar, wird das Bitdefender-Produkt Sie per Pop-up-Benachrichtigung darüber informieren. So können Sie von unseren Vorteilspreisen profitieren und Ihre Geräte länger schützen.

Zudem können Produktbenachrichtigungen angezeigt werden, wenn der Benutzer Veränderungen im Produkt vornimmt.

So können Sie Benachrichtigungen zu Sonderangeboten und dem Produkt aktivieren oder deaktivieren:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Allgemeine Einstellungen** aus.
4. Aktivieren oder deaktivieren Sie Benachrichtigungen zu Sonderangeboten und dem Produkt, indem Sie auf den entsprechenden Schalter klicken.

Die Option für die Benachrichtigungen zu Sonderangeboten und dem Produkt ist standardmäßig aktiviert.



Beachten Sie

Nach der Deaktivierung der Benachrichtigungen zu Sonderangeboten und dem Produkt wird Bitdefender Sie auch weiterhin über Sonderangebote informieren, falls Sie eine Testversion nutzen, Ihre Lizenz in Kürze abläuft oder Sie eine bereits abgelaufene Produktversion nutzen.

5. BITDEFENDER-BENUTZEROBERFLÄCHE

Bitdefender Internet Security 2015 entspricht den Bedürfnissen sowohl von Profis als auch von Beginnern. Die grafische Benutzeroberfläche ist so konzipiert, dass Sie für jeden Benutzer anpassbar ist.

Um den Produktstatus abzurufen und grundlegende Aufgaben auszuführen, steht Ihnen das Bitdefender-Symbol in der Task-Leiste jederzeit zur Verfügung.

Über das Hauptfenster haben Sie Zugriff auf wichtige Produktinformationen und die einzelnen Produktmodule und können die häufigsten Aufgaben erledigen. Über das Hauptfenster können Sie für eine detaillierte Konfiguration und erweiterte Verwaltungsaufgaben auf den Tafelbereich zugreifen und mittels des Autopiloten und der Profile das Produktverhalten konfigurieren.

Wenn Sie wichtige Sicherheitsinformationen ständig im Blick haben und direkten Zugriff auf wichtige Einstellungen haben möchten, können Sie das Sicherheits-Widget zu Ihrem Desktop hinzufügen.

5.1. Task-Leisten-Symbol

Um das gesamte Produkt schneller zu verwalten, können Sie das Bitdefender-Symbol in der Task-Leiste nutzen.

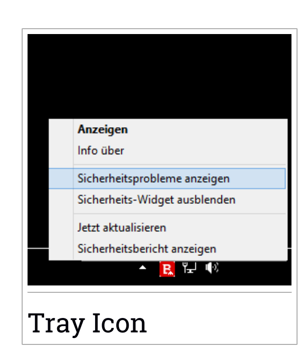


Beachten Sie

Wenn Sie Windows Vista, Windows 7 oder Windows 8 verwenden, ist das Bitdefender-Symbol unter Umständen nicht immer sichtbar. So können Sie das Symbol immer sichtbar halten:

1. Klicken Sie auf den Pfeil in der unteren rechten Ecke des Bildschirms.
2. Klicken Sie auf **Benutzerdefiniert ...**, um das Fenster der Infobereichsymbole zu öffnen.
3. Wählen Sie **Symbole und Benachrichtigungen anzeigen** für das Symbol **Bitdefender Agent**.

Wenn Sie dieses Icon doppelklicken wird sich Bitdefender öffnen. Wird das Symbol mit der rechten Maustaste angeklickt, öffnet sich ein Kontextmenü, mit dem Sie das BitdefenderProdukt verwalten können.



Tray Icon

- **Anzeigen** - Öffnet das Bitdefender-Hauptfenster.
- **Über** - öffnet ein Fenster, in dem Sie Informationen über Bitdefender erhalten und Hilfe finden, falls etwas Unvorhergesehenes geschieht.
- **Sicherheitsprobleme anzeigen** - hilft bestehende Sicherheitsschwachstellen zu entfernen. Falls die Option nicht verfügbar ist, so gibt es keine zu behebenden Probleme. Für weitere Informationen lesen Sie bitte *„Probleme beheben“* (S. 14).
- **Sicherheits-Widget anzeigen/ausblenden** - aktiviert/deaktiviert das Sicherheits-Widget.
- **Jetzt Aktualisieren** - startet ein sofortiges Update. Sie können den Update-Status im Update-Bereich des Bitdefender-Hauptfensters verfolgen.
- **Sicherheitsbericht anzeigen** - Öffnet ein Fenster, in dem ein wöchentlicher Statusbericht sowie Empfehlungen für Ihr System angezeigt werden. Beachten Sie die Empfehlungen, um die Sicherheit Ihres Systems zu verbessern.

Das Bitdefender-Symbol in der System Tray informiert Sie über spezielle Symbole, über mögliche Probleme:

Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.
Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
Der Bitdefender-Autopilot ist aktiviert.

Wenn Bitdefender nicht aktiv ist, ist das Symbol in der Task-Leiste grau hinterlegt: . Dies passiert normalerweise, wenn die Lizenz abgelaufen ist. Es kann auch vorkommen, wenn die Bitdefender Services nicht reagieren oder andere Fehler die normale Funktionsweise von Bitdefender einschränken.

5.2. Hauptfenster

Im Bitdefender-Hauptfenster können Sie die häufigsten Aufgaben durchführen, Sicherheitsprobleme schnell und einfach beheben,

Informationen über die Programmausführung anzeigen und die Produkteinstellungen konfigurieren. Und das alles mit nur wenigen Klicks.

Das Fenster ist in zwei Hauptbereiche aufgeteilt:

Obere Symbolleiste
: Hier können Sie den Sicherheitsstatus Ihres Computers überprüfen, das Bitdefender-Verhalten in bestimmten Situationen konfigurieren und auf wichtige Aufgaben zugreifen.

Tafelbereich
: Hier können Sie die Bitdefender-Hauptmodule verwalten und verschiedene Aufgaben ausführen, um Ihren Computer zu schützen und die Systemgeschwindigkeit zu optimieren.

Über das -Symbol im oberen Bereich des Fensters können Sie Ihr Konto verwalten und über sein Dashboard auf die Online-Funktionen des Produkts zugreifen. Von hier aus können Sie auch die Ereignisse, den wöchentlichen Sicherheitsbericht und die Hilfe & Support-Seite aufrufen.

Link	Beschreibung
Anzahl der verbleibenden Tage	Der Zeitraum, für den Ihre aktuelle Lizenz noch gilt. Wenn Sie auf den Link klicken, wird ein Fenster geöffnet, in dem mehr Informationen über Ihren Lizenzschlüssel angezeigt werden und in dem Sie Ihr Produkt mit einem neuen Lizenzschlüssel registrieren können.
Jetzt kaufen	Unterstützt Sie beim Kauf des Lizenzschlüssels für Ihr Bitdefender Internet Security 2015-Produkt.

5.2.1. Obere Symbolleiste

Die obere Symbolleiste enthält die folgenden Elemente:

- **Sicherheitsstatusbereich** Dieser befindet sich auf der linken Seite der Symbolleiste und enthält Informationen darüber, ob Probleme die Sicherheit Ihres Computers beeinträchtigen und hilft Ihnen, diese zu beheben.

  Die Farbe des Sicherheitsstatusbereichs verändert sich abhängig von den erkannten Problemen. Zudem werden unterschiedliche Meldungen angezeigt:

  - **Der Bereich ist grün markiert.** Es müssen keine Probleme behoben werden. Ihr Rechner und Ihre Daten sind geschützt.

- **Der Bereich ist gelb markiert.** Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
- **Der Bereich ist rot markiert.** Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt. Sie sollten sich umgehend um diese Probleme kümmern.

Mit einem Klick auf eine beliebige Stelle im Sicherheitsstatusbereich können Sie einen Assistenten aufrufen, mit dem Sie alle Bedrohungen einfach und schnell von Ihrem Computer entfernen können. Für weitere Informationen lesen Sie bitte *„Probleme beheben“* (S. 14).

- **Autopilot** Hier können Sie den Autopilot aktivieren und den unauffälligen Hintergrundschutz für sich arbeiten lassen. Für weitere Informationen lesen Sie bitte *„Autopilot“* (S. 18).
- **Profile** Hier können Sie das System so konfigurieren, dass Wartungsaufgaben automatisch verschoben werden, damit Sie unterbrechungsfrei arbeiten, spielen und Filme ansehen können. Für weitere Informationen lesen Sie bitte *„Profile“* (S. 192).

5.2.2. Tafelbereich

Der Tafelbereich ist zweigeteilt, links im Fenster können Sie die Bitdefender-Produktmodule aufrufen und verwalten, rechts können Sie wichtige Aufgaben über die jeweiligen Schaltflächen starten.

In diesem Bereich stehen Ihnen die folgenden Tafeln zur Verfügung:

- Schutz
- Privatsphäre
- Extras
- Schaltflächen

Schutz

In diesem Bereich können Sie die Sicherheitsstufe festlegen, Freunde und Spammer verwalten, Netzwerkverbindungseinstellungen anzeigen und bearbeiten sowie festlegen, welche Schwachstellen im System behoben werden sollen.

Im Bereich Schutz können Sie die folgenden Module verwalten:

Antivirus

Der Virenschutz bildet die Grundlage Ihrer Sicherheit. Bitdefender schützt Sie sowohl in Echtzeit als auch bei Bedarf vor allen Arten von Malware, so zum Beispiel vor Viren, Trojanern, Spyware, Adware usw.

Über das Modul Virenschutz können Sie schnell und einfach auf die folgenden Scan-Aufgaben zugreifen:

- Quick-Scan
- System-Scan
- Scans verwalten
- Rettungsmodus

Weitere Informationen zu den Scan-Aufgaben und eine Anleitung, wie Sie den Virenschutz konfigurieren können, finden Sie im Kapitel *„Virenschutz“* (S. 91).

Firewall

Die Firewall schützt Sie, während Sie mit Netzwerken und dem Internet verbunden sind, indem alle Verbindungsversuche gefiltert werden.

Weitere Informationen zur Firewall-Konfiguration finden Sie im Kapitel *„Firewall“* (S. 141).

Angriffserkennung

Die Angriffserkennung analysiert System- und Netzwerkaktivitäten und sucht dabei nach ungewöhnlichem Verhalten und möglichen Angriffen.

Weitere Informationen, wie man die Angriffserkennung zum Schutz Ihrer System- und Netzwerkaktivitäten konfigurieren kann, finden Sie im Kapitel *„Angriffserkennung“* (S. 151).

Internet-Schutz

Mit dem Internet-Schutz schützen Sie sich beim Surfen zuverlässig vor Phishing-Angriffen, Betrugsversuchen und der unbeabsichtigten Weitergabe privater Daten.

Weitere Informationen, wie man Bitdefender zum Schutz Ihrer Internet-Aktivitäten konfigurieren kann, finden Sie im Kapitel *„Internet-Schutz“* (S. 128).

Antispam

Das Spam-Schutz-Modul von Bitdefender stellt sicher, dass Ihr Posteingang von unerwünschten E-Mails frei bleibt, indem es den POP3-Nachrichtenverkehr filtert.

Weitere Informationen zum Spam-Schutz finden Sie im Kapitel *„Antispam“* (S. 118).

Schwachstelle

Über das Schwachstellen-Modul halten Sie Ihr Betriebssystem und Ihre regelmäßig genutzten Anwendungen auf dem neusten Stand.

Klicken Sie im Modul Schwachstellen auf **Schwachstellen-Scan**, um kritische Windows-Updates, Anwendungs-Updates und schwache Passwörter für Windows-Konten zu identifizieren.

Weitere Informationen zur Konfiguration des Schwachstellenschutzes finden Sie im Kapitel *„Schwachstelle“* (S. 137).

Privatsphäre

Im Bereich Privatsphäre können Sie Ihre persönlichen Daten verschlüsseln, Ihre Online-Transaktionen absichern, für ein sicheres Surf-Vergnügen sorgen und Ihre Kinder schützen, indem Sie ihre Online-Aktivitäten anzeigen und einschränken.

Im Bereich Privatsphäre können Sie die folgenden Module verwalten:

Datenschutz

Mit dem Modul Datenschutz können Sie verhindern, dass Sie private Daten beim Surfen im Internet unbeabsichtigt weitergeben. Zudem können Sie Dateien endgültig löschen.
Klicken Sie im Modul Datenschutz auf **Dateischredder**, um einen Assistenten zu starten, mit dem Sie Dateien endgültig von Ihrem System entfernen können.

Weitere Informationen zur Konfiguration des Datenschutzes finden Sie im Kapitel *„Datenschutz“* (S. 132).

Geldbörse

Die Geldbörse verwaltet Ihre Passwörter und hilft Ihnen, nie wieder ein Passwort zu vergessen. Zudem schützt es Ihre Privatsphäre und garantiert ein sicheres Internet-Vergnügen.

Im Modul Geldbörse können Sie die folgenden Aufgaben auswählen:

- **Geldbörse öffnen** - Öffnet die bestehende Geldbörse-Datenbank.
- **Geldbörse exportieren** - Hiermit können Sie die bestehende Datenbank lokal speichern.

- **Neue Geldbörse anlegen** - Öffnet einen Assistenten, mit dem Sie eine neue Geldbörse-Datenbank anlegen können.

Weitere Informationen über die Konfiguration von Geldbörse finden Sie im Kapitel *„Die Geldbörse schützt Ihre Anmeldedaten“* (S. 157).

Jugendschutz

Mit der Bitdefender-Kindersicherung können Sie die Computer-Nutzung Ihres Kindes jederzeit überwachen. Bei unangemessenen Inhalten können Sie den Zugriff auf das Internet und auf bestimmte Anwendungen einschränken.

Klicken Sie im Modul Kindersicherung auf **Konfigurieren**, um die Windows-Konten Ihrer Kinder zu konfigurieren und Ihre Aktivitäten von überall aus zu überwachen.

Weitere Informationen zur Konfiguration der Kindersicherung finden Sie in Kapitel *„Jugendschutz“* (S. 164).

Safepay

Mit dem Bitdefender Safepay™-Browser können Sie Ihre Online-Bankgeschäfte und -Einkäufe und alle anderen Online-Transaktionen absichern und vor fremden Zugriff schützen.

Klicken Sie im Modul Safepay auf **Safepay öffnen**, um Ihre Online-Transaktionen in einer sicheren Umgebung abzuwickeln.

Weitere Informationen zu Bitdefender Safepay™ finden Sie im Kapitel *„Sichere Online-Transaktionen mit Safepay“* (S. 152).

Extras

Im Bereich Extras können Sie Ihr Arbeitsprofil konfigurieren, die Systemgeschwindigkeit verbessern, wichtige Dateien sichern und den Schutz für Ihr Facebook-Konto verwalten.

Im Bereich Extras können Sie die folgenden Module verwalten:

Safego

Bitdefender Safego ist eine Sicherheitslösung, die eine sichere Online-Umgebung für die Facebook-Nutzung schafft, indem es sowohl Ihre Aktivitäten als auch die Ihrer Freunde überwacht und Sie vor potenziell schädlichen Beiträgen schützt.

Für weitere Informationen lesen Sie bitte *„Safego für Facebook“* (S. 177).

PC-Tuning

Bitdefender Internet Security 2015 bietet Ihnen nicht nur Sicherheit, sondern hilft Ihnen auch dabei, die Leistung Ihres Computers zu verbessern.

Im Modul PC-Tuning können Sie auf eine Reihe nützlicher Werkzeuge zugreifen:

- Ein-Klick-Optimierung
- Systemstartoptimierung
- PC-Bereinigung
- Defragmentierung
- Registry-Bereinigung
- Registry-Wiederherst.
- Dublettensuche

Weitere Informationen zu den Tools zur Leistungsoptimierung finden Sie im Kapitel *„PC-Tuning“* (S. 183).

Profile

Die Bitdefender-Profile überwachen den Produkt- und Systembetrieb und sorgen so für mehr Benutzerfreundlichkeit, wenn Sie arbeiten, spielen oder Filme schauen. Klicken Sie in der oberen Symbolleiste in der Bitdefender-Benutzeroberfläche auf **Jetzt aktivieren**, um diese Funktion zu nutzen.

Mit Bitdefender können Sie die folgenden Profile konfigurieren:

- Arbeitsprofil
- Filmprofil
- Spielprofil

Weitere Informationen zur Konfiguration des Moduls Profile finden Sie in Kapitel *„Profile“* (S. 192).

Schaltflächen

Im Schaltflächenbereich können Sie wichtige Aufgaben im Zusammenhang mit der Sicherheit Ihrer Aktivitäten ausführen. Wenn Sie einen Scan durchführen, das Produkt aktualisieren, Ihre Online-Transaktionen absichern oder Ihre Systemgeschwindigkeit optimieren möchten, stehen Ihnen die folgenden Optionen zur Verfügung:

Scan
Führen Sie einen Quick Scan durch, um sicherzustellen, dass Ihr Computer virenfrei ist.

Update
Aktualisieren Sie Ihr Bitdefender, um sicherzustellen, dass Ihre Malware-Signaturen auf dem neuesten Stand sind.

Safepay
Öffnen Sie Safepay, um Ihre sensiblen Daten bei Online-Transaktionen zu schützen.

Optimieren
Gewinnen Sie Speicherplatz auf der Festplatte, beheben Sie Registry-Fehler und schützen Sie Ihre Privatsphäre, indem Sie nicht mehr benötigte Dateien mit nur einem Klick löschen.

5.3. Die Bitdefender-Module

Das Bitdefender-Produkt verfügt über eine Reihe nützlicher Module, die Sie bei der Arbeit, beim Surfen im Netz oder dem Abwickeln von Online-Zahlungen schützen, Ihre Systemgeschwindigkeit deutlich steigern und viele weitere Funktionen bieten. Wenn Sie auf die Module zugreifen oder Ihr Produkt konfigurieren möchten, müssen Sie in der Bitdefender-Benutzeroberfläche nur auf die Bereiche **Schutz**, **Privatsphäre** und **Extras** klicken.

Die folgende Auflistung beschreibt in Kürze jedes Modul.

Antivirus
Hier können Sie Ihren Malware-Schutz konfigurieren, Scan-Ausschlüsse festlegen und Dateien in Quarantäne verwalten.

Antispam
Bietet Ihnen die Möglichkeit Ihr Postfach SPAM-frei zu halten und die Antispam-Einstellungen detailliert zu konfigurieren.

Internet-Schutz
Hier erfahren Sie, ob die Informationen auf den Webseiten, die Sie aufrufen möchten, sicher sind.

Schwachstelle
Hier können Sie Schwachstellen in Ihrem System aufdecken und beheben.

Datenschutz
Hier können Sie verhindern, dass Daten von Ihrem Computer nach außen gelangen, und Ihre Privatsphäre bei Surfen im Internet schützen.

Firewall
Hier können Sie allgemeine Firewall-Einstellungen vornehmen und Regeln verwalten.

Angriffserkennung
Lässt Sie System- und Netzwerkaktivitäten überwachen und verdächtiges Verhalten und mögliche Angriffe erkennen.

Geldbörse
Ermöglicht Ihnen, mit nur einem Master-Passwort auf alle Anmeldedaten zuzugreifen.

Profile
Hier können Sie Ihr Arbeitsprofil festlegen, um für noch mehr Benutzerfreundlichkeit zu sorgen.

Jugendschutz
Hier können Sie Ihre Kinder gegen jugendgefährdende Inhalte schützen. Nutzen Sie dabei Ihre selbst festgelegten Regeln.

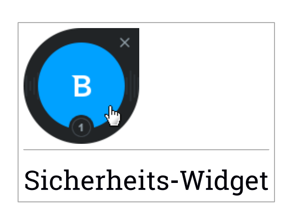
PC-Tuning
Hiermit können Sie die Leistung Ihres Computers und die Ressourcenauslastung überwachen.

5.4. Sicherheits-Widget

Das **Sicherheits-Widget** ist die bequemste und schnellste Art Bitdefender Internet Security 2015 zu steuern. Wenn Sie dieses kleine, unauffällige Widget auf Ihren Desktop legen, haben Sie jederzeit wichtige Informationen im Blick und können zentrale Aufgaben ausführen:

- Öffnet das Bitdefender-Hauptfenster.
- Scan-Activität in Echtzeit überwachen;
- den Sicherheitsstatus Ihres Systems überwachen und gefundene Probleme beheben;
- Zeigt an, wenn ein Update durchgeführt wird.
- Benachrichtigungen und Ereignisprotokolle von Bitdefender lesen;

- Dateien und Ordner (einzeln oder als Gruppe) scannen, indem Sie sie auf das Widget ziehen;



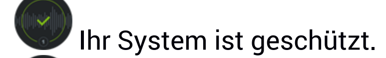
Sicherheits-Widget

Der Gesamtsicherheitsstatus Ihres Computers wird **in der Mitte** des Widgets angezeigt. Farbe und Form des Symbols in der Mitte zeigen unterschiedliche Status an.

Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt.

Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden. Klicken Sie auf das Statussymbol, um die gemeldeten Probleme zu beheben.

Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben. Klicken Sie auf das Statussymbol, um die gemeldeten Probleme zu beheben.



Ihr System ist geschützt.

Während ein Bedarf-Scan läuft, wird dieses animierte Symbol angezeigt.

Wenn Probleme gemeldet werden, klicken Sie auf das Statussymbol, um den Problembehebungsassistenten zu starten.

Im unteren Bereich des Widgets werden die ungelesenen Ereignisse angezeigt (die Anzahl der unbeachteten Ereignisse, die Bitdefender gemeldet hat). Klicken Sie auf den Ereigniszähler, der z. B. bei einem ungelesenen Ereignis so aussieht, um das Ereignisfenster zu öffnen. Für weitere Informationen lesen Sie bitte *„Ereignisanzeige“* (S. 16).

5.4.1. Dateien und Verzeichnis scannen

Mit dem Sicherheits-Widget können Sie ganz einfach Dateien und Ordner scannen. Sie können Dateien und/oder Ordner einfach auf das

Sicherheits-Widget ziehen und dort ablegen, um diese(n) Datei/Ordner zu scannen.

Der Viren-Scan-Assistent wird angezeigt. Er führt Sie durch den Scan-Vorgang. Die Scan-Optionen sind für bestmögliche Erkennungsraten vorkonfiguriert und können nicht verändert werden. Falls infizierte Dateien gefunden werden, wird Bitdefender versuchen, diese zu desinfizieren (den Schad-Code zu entfernen). Wenn die Desinfizierung fehlschlagen sollte, wird Ihnen der Viren-Scan-Assistent andere Möglichkeiten anbieten, wie mit den infizierten Dateien verfahren werden soll.

5.4.2. Das Sicherheits-Widget ausblenden/anzeigen

Wenn Sie das Widget nicht mehr angezeigt bekommen möchten, klicken Sie einfach auf ⊗.

Verwenden Sie eine der folgenden Methoden, um das Sicherheits-Widget wiederherzustellen:

- Über die Task-Leiste:
  1. Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol in der Task-Leiste.
  2. Klicken Sie im daraufhin angezeigten Kontextmenü auf **Sicherheits-Widget anzeigen**.
- Über die Bitdefender-Benutzeroberfläche:
  1. Öffnen Sie das Bitdefender-Fenster.
  2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
  3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Allgemeine Einstellungen** aus.
  4. Aktivieren Sie den **Sicherheits-Widget anzeigen**, indem Sie auf den entsprechenden Schalter klicken.

5.5. Sicherheitsbericht

Der Sicherheitsbericht liefert Ihnen neben einem wöchentlichen Produktstatus verschiedene Tipps zur Verbesserung des Systemschutzes. Diese Tipps sind eine wichtige Hilfe bei der Verwaltung Ihres Schutzes und ermöglichen einen schnellen Überblick über die verfügbaren Aktionen.

Der Bericht wird einmal pro Woche erstellt und fasst alle relevanten Informationen zu den Produktaktivitäten zusammen, um Ihnen einen schnellen Überblick über alle Ereignisse in diesem Zeitraum zu geben.

Die Informationen im Sicherheitsbericht sind in zwei Kategorien unterteilt:

- Der Bereich **Schutz** - Zeigt Informationen zum Thema Systemschutz an.
  - **Geprüfte Spy-Dateien**

    Hier sehen Sie die Dateien, die von Bitdefender im Verlauf der Woche gescannt wurden. Hier können Sie alle Details wie die Anzahl der gescannten Dateien und der von Bitdefender bereinigten Dateien einsehen.

    Weitere Informationen zum Virenschutz finden Sie im Kapitel *„Virenschutz“* (S. 91).
  - **Gescannte Websites**

    Hier können Sie sehen, wie viele Webseiten von Bitdefender gescannt und blockiert wurden. Um Sie vor der Preisgabe von persönlichen Informationen im Internet zu schützen, sichert Bitdefender Ihren Datenverkehr ab.

    Weitere Informationen zum Internet-Schutz finden Sie im Kapitel *„Internet-Schutz“* (S. 128)
  - **Schwachstellen**

    Hier können Sie Systemschwachstellen schnell und einfach identifizieren und beheben, um Ihren Computer besser vor Malware und Hacker-Angriffen zu schützen.

    Weitere Informationen zum Schwachstellen-Scan finden Sie im Kapitel *„Schwachstelle“* (S. 137).
  - **Ereignischronik**

    Hier können Sie sich einen Überblick über alle Scan-Prozesse und von Bitdefender im Laufe der Woche behobenen Probleme verschaffen. Die Ereignisse sind nach Tagen geordnet.

    Weitere Informationen und ein detailliertes Ereignisprotokoll aller Aktivitäten auf Ihrem Computer finden Sie unter Ereignisse.

- **Optimierungs**bereich - Hier erhalten Sie Informationen zu gewonnenen Speicherplatz, optimierten Anwendungen und der Akkulaufzeit, die Sie durch den Akkubetrieb gewonnen haben.
  - **Gewonnener Speicherplatz**

    Hier sehen Sie, wie viel Speicherplatz während der Systemoptimierung gewonnen wurde. Mit dem PC-Tuning verbessert Bitdefender Ihre Systemgeschwindigkeit.

    Weitere Informationen zur TuneUp finden Sie im Kapitel *„PC-Tuning“* (S. 183).
  - **Gewonnene Akkulaufzeit**

    Hier können Sie sehen, wie viel Akkulaufzeit Sie durch den Akkubetrieb gewonnen haben.

    Weitere Informationen zum Akkubetrieb finden Sie im Kapitel *„Akkubetrieb“* (S. 21).
  - **Optimierte Apps**

    Hier sehen Sie die Anzahl der Anwendungen, die Sie im Zusammenhang mit den Profilen verwendet haben.

    Weitere Informationen zur Profile finden Sie im Kapitel *„Profile“* (S. 192).

5.5.1. Aufrufen des Sicherheitsberichts

Der Sicherheitsbericht nutzt ein System zur Problemverfolgung, um potenzielle Sicherheitsprobleme für Ihren Computer und Ihre Daten zu erkennen und Sie darüber zu informieren. Zu den gefundenen Problemen gehören auch wichtige Schutzeinstellungen, die deaktiviert sind, und andere Umstände, die ein Sicherheitsrisiko darstellen. Mithilfe des Berichts können Sie bestimmte Bitdefender-Komponenten konfigurieren oder vorbeugende Maßnahmen ergreifen, um Ihren Computer und Ihre privaten Daten zu schützen.

Um den Sicherheitsbericht aufzurufen, gehen Sie folgendermaßen vor:

1. Den Bericht öffnen:
   - Öffnen Sie das Bitdefender-Fenster, klicken Sie oben im Fenster auf das -Symbol und wählen Sie danach **Sicherheitsbericht** aus dem Menü aus.

- Rechtsklicken Sie auf das Bitdefender-Symbol in der Task-Leiste und wählen Sie **Sicherheitsbericht anzeigen**.
- Sie erhalten eine Pop-up-Benachrichtigung sobald ein Bericht bereitsteht. Klicken Sie auf **Anzeigen**, um den Sicherheitsbericht aufzurufen.

  In Ihrem Browser wird eine Seite geöffnet, auf der Sie den erstellten Bericht einsehen können.

2. Im Fenster oben können Sie den allgemeinen Sicherheitsstatus einsehen.
3. Lesen Sie unsere Empfehlungen unten auf der Seite.

Die Farbe des Sicherheitsstatusbereichs verändert sich abhängig von den erkannten Problemen. Zudem werden unterschiedliche Meldungen angezeigt:

- **Der Bereich ist grün markiert.** Es müssen keine Probleme behoben werden. Ihr Rechner und Ihre Daten sind geschützt.
- **Der Bereich ist gelb markiert.** Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
- **Der Bereich ist rot markiert.** Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt. Sie sollten sich umgehend um diese Probleme kümmern.

5.5.2. Aktivieren oder Deaktivieren der Benachrichtigungen zum Sicherheitsbericht

Um die Benachrichtigungen zum Sicherheitsbericht zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Allgemeine Einstellungen** aus.
4. Klicken Sie auf den entsprechenden Schalter, um die Benachrichtigungen zum Sicherheitsbericht zu aktivieren oder deaktivieren.

   Die Benachrichtigungen zum Sicherheitsbericht sind standardmäßig aktiviert.

6. BITDEFENDER REGISTRIEREN

Damit Bitdefender Sie schützen kann, müssen Sie Ihr Produkt mit einem Lizenzschlüssel registrieren. Die Lizenzschlüssel legt fest, für wie lange Sie das Produkt einsetzen können. Sobald der Lizenzschlüssel abgelaufen ist, wird Bitdefender alle Funktionen und somit den Schutz Ihres Computers einstellen.

Sie sollten einige Tage bevor die momentan genutzte Lizenz abläuft diese verlängern oder eine neue erwerben. Für weitere Informationen lesen Sie bitte *„Kaufen oder Erneuern von Lizenzschlüsseln“* (S. 41). Falls Sie eine Testversion von Bitdefender nutzen, müssen Sie diese mit einem Lizenzschlüssel registrieren, wenn Sie die Software auch nach Ablauf der Testphase weiterhin nutzen wollen.

6.1. Eingeben des Lizenzschlüssels

Wenn Sie sich bei der Installation für die Testversion entschieden haben, steht diese Ihnen 30 Tage lang zur Verfügung. Um Bitdefender auch nach Ablauf der Testphase weiterhin nutzen zu können, müssen Sie das Produkt mit einem Lizenzschlüssel registrieren.

Im unteren Bereich des Bitdefender-Fensters zeigt ein Link an, wie viele Tage Ihre Lizenz noch gültig ist. Klicken Sie auf diesen Link, um das Registrierungsfenster zu öffnen.

Sie sehen den Registrierungsstatus von Bitdefender sehen, den aktuellen Lizenzschlüssel und wieviele Tage verbleiben, bis die Lizenz abläuft.

Um Bitdefender Internet Security 2015 zu registrieren:

1. Geben Sie den Lizenzschlüssel in das entsprechende Feld ein.



Beachten Sie

Sie finden den Lizenzschlüssel:
- Auf dem CD-Aufdruck.
- auf dem Lizenzzertifikat.
- In der E-Mail-Bestätigung des Online-Kaufs.

Falls Sie über keinen Bitdefender-Lizenzschlüssel verfügen, klicken Sie auf den Link, der Ihnen in dem Fenster angezeigt wird. Dieser ruft eine Website auf, über die Sie einen Schlüssel erwerben können.

2. Klicken Sie auf **Jetzt registrieren**.

Auch wenn Sie bereits einen Lizenzschlüssel erworben haben, wird Bitdefender Internet Security 2015 weiter als Testversion angezeigt, bis Sie die Registrierung des Produkts abgeschlossen haben.

6.2. Kaufen oder Erneuern von Lizenzschlüsseln

Wenn sich die Testperiode dem Ende zuneigt, sollten Sie einen Lizenzschlüssel erwerben und Ihr Produkt registrieren. Falls Ihr aktueller Lizenzschlüssel in Kürze abläuft, müssen Sie Ihre Lizenz verlängern.

Bitdefender wird Sie benachrichtigen, wenn das Ablaufdatum Ihrer aktuellen Lizenz näher rückt. Befolgen Sie die Anweisungen in der Benachrichtigung, um eine neue Lizenz zu erwerben.

Sie können zudem jederzeit eine Website aufrufen, über die Sie einen Lizenzschlüssel erwerben können. Gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie im unteren Bereich des Bitdefender-Fensters auf den Link, der die verbleibenden Tage der Lizenz anzeigt, um das Fenster für die Produktregistrierung zu öffnen.
3. Klicken Sie auf **Sie haben keinen Lizenzschlüssel? Erwerben Sie einen.**
4. In Ihrem Browser öffnet sich eine Webseite, auf der Sie einen Bitdefender-Lizenzschlüssel erwerben können.

7. MYBITDEFENDER-KONTO

Die Online-Funktionen Ihres Produkts sowie einige zusätzliche Bitdefender-Dienste stehen nur über ein MyBitdefender-Konto zur Verfügung. Dazu müssen Sie Ihren Computer mit MyBitdefender verknüpfen, indem Sie sich aus Bitdefender Internet Security 2015 heraus bei einem Konto anmelden. Die zusätzlichen Funktionen und Dienste sind:

- Ihren Lizenzschlüssel abrufen, sollten Sie ihn verloren haben.
- die Einstellungen der Kindersicherung für die Windows-Konten Ihrer Kinder konfigurieren und deren Aktivität auf dem Rechner überwachen, auch wenn Sie nicht zu Hause sind.
- Ihr Facebook-Konto mit Safego schützen.
- Fernverwaltung von Bitdefender Internet Security 2015.

MyBitdefender lässt sich mit den verschiedensten Bitdefender-Sicherheitslösungen für PCs und andere Plattformen nutzen. Sie können die Sicherheit aller Geräte, die mit Ihrem Konto verknüpft sind, über ein zentrales Dashboard verwalten.

Sie können auf Ihr MyBitdefender-Konto von jedem Gerät mit Internetzugang aus zugreifen. Rufen Sie dazu einfach https://my.bitdefender.com auf.

Sie können Ihr Konto auch direkt aus Ihrem Bitdefender-Produkt heraus öffnen und verwalten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **MyBitdefender** aus dem Menü aus.

7.1. Den Computer mit MyBitdefender verknüpfen

Um Ihren Computer mit einem MyBitdefender-Konto zu verknüpfen, müssen Sie sich bei einem Konto von Bitdefender Internet Security 2015 aus anmelden. Bis Sie Ihren Computer mit MyBitdefender verknüpft haben, werden Sie immer, wenn Sie eine Funktion nutzen möchten, die ein Konto erfordert, aufgefordert, sich bei Ihrem MyBitdefender-Konto anzumelden.

So öffnen Sie das Fenster, in dem Sie ein MyBitdefender-Konto erstellen oder sich bei einem bestehenden Konto anmelden können:

1. Öffnen Sie das Bitdefender-Fenster.

2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Kontodetails** aus dem Menü aus.

   Wenn Sie sich bereits bei einem Konto angemeldet haben, wird dieses Konto angezeigt. Klicken Sie auf **Mit einem anderen Konto anmelden**, um den Computer mit einem anderen Benutzerkonto zu verknüpfen.

Wenn Sie sich bereits bei einem Konto angemeldet haben, wird dieses Konto angezeigt. Klicken Sie auf **Zu MyBitdefender**, um Ihr Dashboard aufzurufen. Um das mit dem Computer verknüpfte Benutzerkonto zu ändern, klicken Sie auf **Mit einem anderen Konto anmelden**.

Wenn Sie sich noch nicht bei einem Konto angemeldet haben, gehen Sie je nach Ihrer Situation vor.

Ich möchte ein MyBitdefender-Konto anlegen

Um ein MyBitdefender-Konto erfolgreich anzulegen, gehen Sie folgendermaßen vor:

1. Wählen Sie **Benutzerkonto anlegen**.

   Ein neues Fenster wird sich öffnen.

2. Geben Sie die Daten in die entsprechenden Felder ein. Die hier eingetragenen Daten bleiben vertraulich.
   - **E-Mail** - Geben Sie Ihre E-Mail-Adresse an.
   - **Benutzername** - Geben Sie einen Benutzernamen für Ihr Konto ein.
   - **Passwort** - Geben Sie ein Passwort für Ihr Benutzerkonto ein. Das Passwort muss mindestens 6 Zeichen lang sein.
   - **Passwort bestätigen** - Geben Sie das Passwort erneut ein.
3. Klicken Sie auf **Erstellen**.
4. Bevor Sie Ihr Konto nutzen können, müssen Sie zunächst die Registrierung abschließen. Rufen Sie Ihre E-Mails ab und folgen Sie den Anweisungen in der Bestätigungsnachricht, die Sie von Bitdefender erhalten haben.

Ich möchte mich über mein Microsoft-, Facebook- oder Google-Konto anmelden

Um sich über Ihr Microsoft-, Facebook- oder Google-Konto anzumelden, gehen Sie folgendermaßen vor:

1. Klicken Sie auf das Symbol für den Dienst, über den Sie sich anmelden wollen. Sie werden auf die Anmeldeseite dieses Dienstes weitergeleitet.
2. Folgen Sie den Anweisungen des ausgewählten Dienstes, um Ihr Benutzerkonto mit Bitdefender zu verknüpfen.



Beachten Sie
Bitdefender hat keinen Zugriff auf Ihre vertraulichen Informationen, so zum Beispiel das Passwort, das Sie zur Anmeldung an Ihrem Konto verwenden, oder die persönlichen Informationen Ihrer Freunde und Kontakte.

Ich habe bereits ein MyBitdefender-Konto

Wenn Sie bereits ein Konto haben, aber dort nicht angemeldet sind, melden Sie sich folgendermaßen an:

1. Geben Sie die E-Mail-Adresse und das Kennwort Ihres Kontos in die entsprechenden Felder ein.

   Beachten Sie
   Falls Sie Ihr Passwort vergessen haben, klicken Sie auf **Passwort vergessen** und folgen Sie den Anweisungen, um ein neues Passwort anzufordern.

2. Klicken Sie auf **Bei MyBitdefender anmelden**.

Sobald der Computer mit einem Konto verknüpft ist, können Sie sich auf https://my.bitdefender.com mit der angegebenen E-Mail-Adresse und dem entsprechenden Passwort anmelden.

Sie können Ihr Konto auch direkt aus Bitdefender Internet Security 2015 aufrufen, indem Sie auf das -Symbol oben im Fenster klicken und **MyBitdefender** aus dem Menü auswählen.

8. BITDEFENDER AUF DEM NEUESTEN STAND HALTEN

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie das Programm Bitdefender stets mit den neuesten Virensignaturen betreiben.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet Bitdefender eigenständig. Standardmäßig sucht die Software nach Updates, wenn Sie Ihren Computer einschalten und danach einmal pro **Stunde**. Wenn ein neues Update erkannt wird, wird es automatisch auf Ihren PC heruntergeladen und installiert.

Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet die entsprechenden Dateien stufenweise aktualisiert werden. So stört der Update-Vorgang nicht den Betrieb des Produkts, während gleichzeitig alle Schwachstellen behoben werden.



Wichtig

Um immer vor den neuesten Bedrohungen geschützt zu sein, sollte das automatische Update immer aktiviert bleiben.

In manchen Situationen kann es notwendig werden, dass Sie eingreifen, um den Bitdefender-Schutz auf dem neuesten Stand zu halten:

- Wenn Ihr Computer über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen wie unter *„Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung?“* (S. 83) beschrieben konfigurieren.
- Wenn Sie über keine Internet-Verbindung verfügen, können Sie Bitdefender, wie im Kapitel *„Mein Computer ist nicht mit dem Internet verbunden. Wie kann ich Bitdefender aktualisieren?“* (S. 211) beschrieben, auch manuell aktualisieren. Die Datei für das manuelle Update wird einmal pro Woche veröffentlicht.
- Bei einer langsamen Internetverbindung können Fehler beim Herunterladen von Updates auftreten. Um zu erfahren, wie Sie solche Fehlern vermeiden können, lesen Sie bitte das Kapitel *„Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann“* (S. 210).

- Falls Sie sich per Einwahl mit dem Internet verbinden, ist es sinnvoll, regelmäßig ein manuelles Bitdefender-Update durchzuführen. Für weitere Informationen lesen Sie bitte *„Durchführung eines Updates“* (S. 46).

8.1. Überprüfen, ob Bitdefender auf dem neuesten Stand ist

Um zu überprüfen, ob Ihr Bitdefender-Schutz auf dem neuesten Stand ist, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Sehen Sie im **Sicherheitsstatusbereich** auf der linken Seite der Task-Leiste nach, wann das letzte Update durchgeführt wurde.

Um ausführliche Informationen zu Ihren letzten Updates zu erhalten, rufen Sie die Update-Ereignisse auf:

1. Klicken Sie im Hauptfenster oben auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.
2. Wählen Sie im Fenster **Ereignisanzeige Update** aus dem entsprechenden Menü aus.

Sie können herausfinden, wann Updates angestoßen wurden und weitere Informationen dazu einholen (d.h. ob sie erfolgreich waren oder nicht, ob ein Neustart erforderlich ist, um die Installation abzuschließen). Falls nötig starten Sie das System sobald es Ihnen möglich ist neu.

8.2. Durchführung eines Updates

Sie benötigen eine Internet-Verbindung, um Updates durchzuführen.

Sie haben folgende Möglichkeiten, ein Update zu starten:

- Öffnen Sie das Bitdefender-Fenster und klicken Sie rechts im Fenster auf die Schaltfläche **Update**.
- Rechtsklicken Sie in der Task-Leiste auf das -Bitdefender-Symbol und wählen Sie **Jetzt aktualisieren**.

Das Update-Modul verbindet sich mit dem Bitdefender-Update-Server und sucht nach verfügbaren Updates. Wenn ein Update erkannt wird, werden Sie abhängig von den Update-Einstellungen entweder aufgefordert, dies zu bestätigen oder das Update wird automatisch durchgeführt.



Wichtig

Möglicherweise kann ein Neustart nach dem vollständig durchgeführten Update notwendig werden. Wir empfehlen, das so bald wie möglich zu tun.

8.3. Aktivieren / Deaktivieren der automatischen Updates

Um das automatische Update zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Update** aus.
4. Klicken Sie auf den Schalter, um automatische Updates zu aktivieren oder deaktivieren.
5. Ein Fenster mit einer Warnung wird eingeblendet. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange die automatischen Updates deaktiviert bleiben sollen. Zur Verfügung stehen die Optionen 5, 15 oder 30 Minuten, eine Stunde, permanent oder bis zum nächsten Systemstart.



Warnung

Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen, die automatischen Updates so kurz wie möglich zu deaktivieren. Denn Bitdefender kann Sie nur dann gegen die neusten Bedrohungen schützen, wenn es auf dem neuesten Stand ist.

8.4. Update-Einstellungen anpassen

Updates können im lokalen Netzwerk, über das Internet, direkt oder durch einen Proxy-Server durchgeführt werden. Standardmäßig scannt Bitdefender jede Stunde auf neue Updates und installiert diese ohne Ihr Zutun.

Die standardmäßigen Update-Einstellungen eignen sich für die meisten Benutzer und es ist normalerweise nicht erforderlich, diese zu ändern.

Um die Update-Einstellungen anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.

2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Update** aus und passen Sie die Einstellungen Ihren Anforderungen an.

Update-Server

Bitdefender ist so konfiguriert, dass Updates von den Bitdefender-Update-Servern aus dem Internet heruntergeladen werden. Die Update-Adresse ist eine generische Internetadresse, die automatisch zu dem Bitdefender-Update-Server, der sich am nächsten zu Ihrem Standort befindet, umgeleitet wird.

Verändern Sie die Update-Adresse nicht, es sei denn, Sie werden von einem Bitdefender-Mitarbeiter oder Ihrem Netzwerkadministrator (falls Sie mit einem Unternehmensnetzwerk verbunden sind) ausdrücklich dazu aufgefordert.

Klicken Sie auf **Standard**, um die ursprüngliche Update-Adresse wiederherzustellen.

Update-Verarbeitungsregeln

Es gibt drei Möglichkeiten, Updates herunterzuladen und zu installieren:

- **Update im Hintergrund** - Bitdefender Updates werden automatisch heruntergeladen und installiert.
- **Vor dem Download nachfragen** - Sobald ein Update verfügbar ist, werden Sie gefragt, ob es heruntergeladen werden soll.
- **Vor der Installation nachfragen** - Sobald ein Update heruntergeladen wurde, werden Sie gefragt, ob die Installation durchgeführt werden soll.

Manche Updates erfordern einen Neustart, um die Installation abzuschließen. Sollte ein Update einen Neustart erforderlich machen, arbeitet Bitdefender standardmäßig mit den alten Dateien weiter, bis der Benutzer den Computer aus eigenen Stücken neu startet. Dadurch soll verhindert werden, dass der Update-Prozess von Bitdefender den Benutzer in seiner Arbeit behindert.

Wenn Sie eine Meldung erhalten möchten, sobald ein Update einen Neustart erfordert, deaktivieren Sie die Option **Neustart verschieben**, indem Sie auf den entsprechenden Schalter klicken.

GEWUSST WIE

9. INSTALLATION

9.1. Wie installiere ich Bitdefender auf einem zweiten Computer?

Wenn Sie einen Lizenzschlüssel für mehrere Computer erworben haben, können Sie denselben Lizenzschlüssel benutzen, um einen weiteren Computer zu registrieren.

So installieren Sie Bitdefender auf einem zweiten Computer:

1. Installieren Sie Bitdefender von der CD/DVD oder über den beim Online-Kauf in der Bestätigungs-E-Mail enthaltenen Installer. Der Installationsvorgang ist in beiden Fällen der gleiche.

   Zu Beginn der Installation werden Sie aufgefordert, die neuesten Installationsdateien herunterzuladen.

2. Geben Sie im eingeblendeten Registrierungsfenster den Lizenzschlüssel ein, und klicken Sie auf **Jetzt registrieren**.

3. Im nächsten Schritt können Sie sich bei Ihrem MyBitdefender-Konto anmelden oder ein neues MyBitdefender-Konto erstellen.

   Sie können Ihr MyBitdefender-Konto auch später erstellen.

4. Warten Sie, bis die Registrierung abgeschlossen ist und schließen Sie dann das Fenster.

9.2. Wann sollte ich Bitdefender neu installieren?

Es gibt Situationen, die es erforderlich machen könnten, dass Sie Ihr Bitdefender-Produkt erneut installieren.

Die Folgenden sind typische Situationen, in denen Sie Bitdefender erneut installieren müssen:

- Sie haben das Betriebssystem neu installiert..
- Sie haben einen neuen Computer erworben..
- Sie wollen die Anzeigesprache der Bitdefender-Benutzeroberfläche ändern..

Um Bitdefender neu zu installieren, können Sie die von Ihnen erworbene Installations-CD verwenden oder eine neue Version von der Bitdefender-Website herunterladen.

Während der Installation werden Sie aufgefordert, das Produkt mit Ihrem Lizenzschlüssel zu registrieren.

Falls Sie Ihren Lizenzschlüssel verloren haben, können Sie sich unter https://my.bitdefender.com bei Ihrem Benutzerkonto anmelden, um ihn abzurufen. Geben Sie die E-Mail-Adresse und das Kennwort Ihres Kontos in die entsprechenden Felder ein.

Weitere Information zum Bitdefender-Installationsprozess finden Sie im Kapitel *„Installieren Ihres Bitdefender-Produkts“* (S. 5).

9.3. Wo kann ich mein Bitdefender-Produkt herunterladen?

Sie können Ihr Bitdefender-Produkt von einer unserer autorisierten Websites(so z.B. von einer Bitdefender-Partner-Website oder einem Online-Shop) oder unserer Website unter http://www.bitdefender.de/Downloads/ herunterladen.



Beachten Sie

Bevor Sie das Installationspaket ausführen, sollten Sie jede andere auf Ihrem System installierte Virenschutzlösung entfernen. Wenn Sie mehr als eine Sicherheitslösung auf Ihrem Computer verwenden, wird dadurch das System instabil.

Um Bitdefender zu installieren, gehen Sie folgendermaßen vor:

1. Doppelklicken Sie auf das heruntergeladene Installationsprogramm und befolgen Sie die Installationsanweisungen.
2. Geben Sie im eingeblendeten Registrierungsfenster den Lizenzschlüssel ein, und klicken Sie auf **Jetzt registrieren**.
3. Im nächsten Schritt können Sie sich bei Ihrem MyBitdefender-Konto anmelden oder ein neues MyBitdefender-Konto erstellen.

   Sie können Ihr MyBitdefender-Konto auch später erstellen.
4. Warten Sie, bis die Registrierung abgeschlossen ist und schließen Sie dann das Fenster.

9.4. Wie wechsle ich von einem Bitdefender-Produkt zu einem anderen?

Der Wechsel von einem Bitdefender-Produkt auf ein anderes ist ganz einfach.

Die drei Bitdefender-Produkte, die Sie auf Ihrem System installieren können, sind:

- Bitdefender Antivirus Plus 2015
- Bitdefender Internet Security 2015
- Bitdefender Total Security 2015

Falls Sie für das gewünschte Produkt keinen Lizenzschlüssel haben, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie im unteren Bereich des Bitdefender-Fensters auf den Link, der die verbleibenden Tage der Lizenz anzeigt, um das Fenster für die Produktregistrierung zu öffnen.
3. Klicken Sie auf **Sie haben keinen Lizenzschlüssel? Erwerben Sie einen.**
4. In Ihrem Browser öffnet sich eine Webseite, auf der Sie einen Bitdefender-Lizenzschlüssel erwerben können.

Nach Erwerb des Lizenzschlüssels für das gewünschte Bitdefender-Produkt, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Im unteren Bereich des Bitdefender-Fensters zeigt ein Link an, wie viele Tage Ihre Lizenz noch gültig ist.

   Klicken Sie auf diesen Link, um das Registrierungsfenster zu öffnen.
3. Geben Sie den neuen Lizenzschlüssel ein und klicken Sie auf **Jetzt registrieren**.
4. Sie werden informiert, dass der Lizenzschlüssel zu einem anderen Bitdefender-Produkt gehört.

   Klicken Sie auf den entsprechenden Link und folgen Sie den Anweisungen, um die Installation durchzuführen.

9.5. Wie verfahre ich mit meinem Bitdefender-Lizenzschlüssel nach einem Windows-Upgrade?

Diese Situation tritt ein, wenn Sie Ihr Betriebssystem aktualisieren und Sie Ihren Bitdefender-Lizenzschlüssel weiterhin nutzen möchten.

Sollten Sie eine vorausgegangene Bitdefender-Version nutzen, können Sie ein kostenloses Upgrade auf die neueste Version von Bitdefender wie folgt durchführen:

- Von einer Vorgängerversion von Bitdefender Antivirus auf die aktuelle Version von Bitdefender Antivirus.
- Von einer Vorgängerversion von Bitdefender Internet Security auf die aktuelle Version von Bitdefender Internet Security.
- Von einer Vorgängerversion von Bitdefender Total Security auf die aktuelle Version von Bitdefender Total Security.

Hierbei gibt es zwei Szenarien:

- Sie haben Ihr Betriebssystem über Windows Update aktualisiert und bemerken, dass Bitdefender nicht mehr funktioniert.

  In diesem Fall müssen Sie das Produkt in der aktuellsten Version erneut installieren.

  Gehen Sie dabei folgendermaßen vor:

  1. Entfernen Sie Bitdefender, indem Sie wie folgt vorgehen:
     - In **Windows XP**:
       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme hinzufügen/entfernen**.
       b. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Entfernen**.
       c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.
       d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
     - Für **Windows Vista** und **Windows 7**:

a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.

b. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.

c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- In **Windows 8**:

a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

c. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.

d. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

e. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

2. Laden Sie die Installationsdatei für die Produktversion herunter, für die Sie einen gültigen Lizenzschlüssel besitzen.

   Sie können das Installationspaket von der Bitdefender Webseite unter folgender Adresse herunterladen: http://www.bitdefender.de/Downloads/.

3. Doppelklicken Sie auf das Installationsprogramm, um den Installationsvorgang zu starten.

4. Geben Sie im eingeblendeten Registrierungsfenster den Lizenzschlüssel ein, und klicken Sie auf **Jetzt registrieren**.

5. Im nächsten Schritt können Sie sich bei Ihrem **MyBitdefender**-Konto anmelden oder ein neues **MyBitdefender**-Konto erstellen.

   Sie können Ihr **MyBitdefender**-Konto auch später erstellen.

Warten Sie, bis die Registrierung abgeschlossen ist und schließen Sie dann das Fenster.

- Sie haben Ihr System gewechselt und möchten nicht auf den Bitdefender-Schutz verzichten.

  Deshalb müssen Sie das Produkt in der aktuellsten Version erneut installieren.

  Gehen Sie dabei folgendermaßen vor:

  1. Laden Sie die Installationsdatei für die Produktversion herunter, für die Sie einen gültigen Lizenzschlüssel besitzen.

     Sie können das Installationspaket von der Bitdefender Webseite unter folgender Adresse herunterladen: http://www.bitdefender.de/Downloads/.
  2. Doppelklicken Sie auf das Installationsprogramm, um den Installationsvorgang zu starten.
  3. Geben Sie im eingeblendeten Registrierungsfenster den Lizenzschlüssel ein, und klicken Sie auf **Jetzt registrieren**.
  4. Im nächsten Schritt können Sie sich bei Ihrem **MyBitdefender**-Konto anmelden oder ein neues **MyBitdefender**-Konto erstellen.

     Sie können Ihr **MyBitdefender**-Konto auch später erstellen.

     Warten Sie, bis die Registrierung abgeschlossen ist und schließen Sie dann das Fenster.

  Weitere Information zum Bitdefender-Installationsprozess finden Sie im Kapitel *„Installieren Ihres Bitdefender-Produkts“* (S. 5).

9.6. Wie kann ich Bitdefender reparieren?

Um Ihr Bitdefender Internet Security 2015 über das Windows-Startmenü zu reparieren, gehen Sie folgendermaßen vor:

- Für **Windows XP**, **Windows Vista** und **Windows 7**:

  1. Klicken Sie auf **Start** und **Alle Programme**.
  2. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.
  3. Klicken Sie im angezeigten Fenster auf **Reparieren**.

Dies kann einige Minuten in Anspruch nehmen.

4. Sie müssen den Computern neu starten, um den Vorgang abzuschließen.

- In **Windows 8**:

1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
3. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.
4. Klicken Sie im angezeigten Fenster auf **Reparieren**.

   Dies kann einige Minuten in Anspruch nehmen.
5. Sie müssen den Computern neu starten, um den Vorgang abzuschließen.

10. REGISTRIERUNG

10.1. Welches Bitdefender-Produkt nutze ich?

Um zu erfahren, welche Bitdefender-Anwendung bei Ihnen installiert ist, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Am oberen Rand des Fensters sollten Sie einen der folgenden Schriftzüge sehen:
   - Bitdefender Antivirus Plus 2015
   - Bitdefender Internet Security 2015
   - Bitdefender Total Security 2015

10.2. Wie kann ich eine Testversion registrieren?

Wenn Sie eine Testversion installiert haben, können Sie diese nur für einen begrenzten Zeitraum benutzen. Um Bitdefender auch nach Ablauf der Testphase weiterhin nutzen zu können, müssen Sie das Produkt mit einem Lizenzschlüssel registrieren.

Um Bitdefender zu registrieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Im unteren Bereich des Bitdefender-Fensters zeigt ein Link an, wie viele Tage Ihre Lizenz noch gültig ist.

   Klicken Sie auf diesen Link, um das Registrierungsfenster zu öffnen.
3. Geben Sie den Lizenzschlüssel ein und klicken Sie auf **Jetzt registrieren**.

   Wenn Sie keinen Lizenzschlüssel haben, klicken Sie in dem Fenster auf den entsprechenden Link. Dieser führt Sie auf eine Website, auf der Sie einen Lizenzschlüssel erwerben können.
4. Warten Sie bis der Registrierungsvorgang abgeschlossen ist und schließen Sie dann das Fenster.

10.3. Wann läuft der Bitdefender-Schutz aus?

Um herauszufinden, wie viele Tage Ihr Lizenzschlüssel noch gültig ist, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Im unteren Bereich des Bitdefender-Fensters zeigt ein Link an, wie viele Tage Ihre Lizenz noch gültig ist.
3. Weitere Informationen erhalten Sie über einen Klick auf den Link, der das Registrierungsfenster öffnet.
4. Im Fenster **Registrieren Sie Ihr Produkt** können Sie:
   - den aktuellen Lizenzschlüssel sehen;
   - einen anderen Lizenzschlüssel eingeben;
   - einen Lizenzschlüssel erwerben.

10.4. Wie verlängere ich meinen Bitdefender-Schutz?

Wenn Ihr Bitdefender-Schutz auszulaufen droht, müssen Sie Ihren Lizenzschlüssel erneuern.

- Um eine Website aufzurufen, auf der Sie Ihren Bitdefender-Lizenzschlüssel erneuern können, gehen Sie folgendermaßen vor:
  1. Öffnen Sie das Bitdefender-Fenster.
  2. Im unteren Bereich des Bitdefender-Fensters zeigt ein Link an, wie viele Tage Ihre Lizenz noch gültig ist. Klicken Sie auf diesen Link, um das Registrierungsfenster zu öffnen.
  3. Klicken Sie auf **Sie haben keinen Lizenzschlüssel? Erwerben Sie einen.**
  4. In Ihrem Browser öffnet sich eine Webseite, auf der Sie einen Bitdefender-Lizenzschlüssel erwerben können.

  Beachten Sie

  Alternativ können Sie auch den Einzelhändler kontaktieren, von dem Sie Ihr Bitdefender-Produkt erworben haben.

- Um Ihr Bitdefender-Produkt mit dem neuen Lizenzschlüssel zu registrieren, gehen Sie folgendermaßen vor:
  1. Öffnen Sie das Bitdefender-Fenster.
  2. Im unteren Bereich des Bitdefender-Fensters zeigt ein Link an, wie viele Tage Ihre Lizenz noch gültig ist. Klicken Sie auf diesen Link, um das Registrierungsfenster zu öffnen.

3. Geben Sie den Lizenzschlüssel ein und klicken Sie auf **Jetzt registrieren**.
4. Warten Sie bis der Registrierungsvorgang abgeschlossen ist und schließen Sie dann das Fenster.

Wenn Sie weitere Informationen benötigen, kontaktieren Sie den Bitdefender-Support wie in Abschnitt *„Hilfe anfordern*“ (S. 238) beschrieben.

11. MYBITDEFENDER

11.1. Wie melde ich mit einem anderen Benutzerkonto bei MyBitdefender an?

Sie haben ein neues MyBitdefender-Konto angelegt und möchten es von nun an nutzen.

Um ein anderes Benutzerkonto nutzen zu können, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Kontodetails** aus dem Menü aus.

   Wenn Sie sich bereits bei einem Konto angemeldet haben, wird dieses Konto angezeigt. Klicken Sie auf **Mit einem anderen Konto anmelden**, um den Computer mit einem anderen Benutzerkonto zu verknüpfen.

   Ein neues Fenster wird sich öffnen.
3. Geben Sie die E-Mail-Adresse und das Kennwort Ihres Kontos in die entsprechenden Felder ein.
4. Klicken Sie auf **Bei MyBitdefender anmelden**

11.2. Wie hinterlege ich eine andere E-Mail-Adresse für mein MyBitdefender-Konto?

Sie haben ein MyBitdefender-Konto mit einer E-Mail-Adresse angelegt, die Sie nicht mehr verwenden, und möchten diese nun ändern.

Die E-Mail-Adresse kann nicht geändert werden, aber Sie können eine andere E-Mail-Adresse nutzen, um ein neues Benutzerkonto anzulegen.

Um ein neues MyBitdefender-Konto anzulegen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Kontodetails** aus dem Menü aus.

Wenn Sie sich bereits bei einem Konto angemeldet haben, wird dieses Konto angezeigt. Klicken Sie auf **Mit einem anderen Konto anmelden**, um den Computer mit einem anderen Benutzerkonto zu verknüpfen.

Ein neues Fenster wird sich öffnen.

3. Wählen Sie **Benutzerkonto anlegen**.
4. Geben Sie die erforderlichen Informationen in die entsprechenden Felder ein. Die hier eingetragenen Daten bleiben vertraulich.
   - **E-mail** - Geben Sie Ihre E-Mail-Adresse an.
   - **Benutzername** - Geben Sie einen Benutzernamen für Ihr Konto ein.
   - **Passwort** - Geben Sie ein Passwort für Ihr Benutzerkonto ein. Das Passwort muss mindestens 6 Zeichen lang sein.
   - **Passwort bestätigen** - Geben Sie das Passwort erneut ein.
   - Klicken Sie auf **Erstellen**.
5. Bevor Sie Ihr Konto nutzen können, müssen Sie zunächst die Registrierung abschließen. Rufen Sie Ihre E-Mails ab und folgen Sie den Anweisungen in der Bestätigungsnachricht, die Sie von Bitdefender erhalten haben.

Verwenden Sie die neue E-Mail-Adresse, um sich bei MyBitdefender anzumelden.

11.3. Wie setzte ich das Passwort für mein MyBitdefender-Konto zurück?

Um ein neues Passwort für Ihr MyBitdefender-Konto festzulegen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Kontodetails** aus dem Menü aus.

   Ein neues Fenster wird sich öffnen.
3. Klicken Sie auf den Link **Mein Passwort vergessen**.
4. Geben Sie die E-Mail-Adresse ein, mit der Sie Ihr MyBitdefender-Konto angelegt haben, und klicken Sie auf **Passwort vergessen**.
5. Rufen Sie Ihre E-Mails ab und klicken Sie auf den entsprechenden Link.

Ein neues Fenster wird sich öffnen.

6. Geben Sie das neue Passwort ein. Das Passwort muss mindestens 6 Zeichen lang sein.
7. Geben Sie das Passwort im Feld **Passwort wiederholen** erneut ein.
8. Klicken Sie auf **Senden**.

Geben Sie Ihre E-Mail-Adresse und das neue Passwort ein, um auf Ihre MyBitdefender-Konto zuzugreifen.

12. PRÜFEN MIT BITDEFENDER

12.1. Wie kann ich eine Datei oder einen Ordner scannen?

Um eine Datei oder einen Ordner einfach und schnell zu scannen, klicken Sie mit der rechten Maustaste auf das Objekt, das Sie scannen möchten, wählen Sie Bitdefender und anschießend **Mit Bitdefender scannen** aus dem Menü.

Um den Scan abzuschließen, folgen Sie den Anweisungen des Scan-Assistenten. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.

Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Typische Situationen, für die diese Scan-Methode geeignet ist:

- Sie vermuten, dass eine bestimmte Datei oder ein Ordner infiziert ist.
- Immer dann, wenn Sie aus dem Internet Dateien herunterladen, von deren Ungefährlichkeit Sie nicht überzeugt sind.
- Scannen Sie einen freigegebenen Ordner, bevor Sie die enthaltenen Dateien auf Ihren Rechner kopieren.

12.2. Wie scanne ich mein System?

Um einen vollständigen System-Scan durchzuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Wählen Sie im Modul **Virenschutz System-Scan** aus.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.

   Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen. Für weitere Informationen lesen Sie bitte *„Viren-Scan-Assistent“* (S. 103).

12.3. Wie kann ich eine benutzerdefinierte Scan-Aufgabe anlegen?

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierte Scan-Aufgabe konfigurieren und ausführen.

Um eine benutzerdefinierte Scan-Aufgabe anzulegen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Wählen Sie im Modul **Virenschutz Scans verwalten** aus.
4. Klicken Sie auf **Neue benutzerdefinierte Aufgabe**, um einen Namen für den Scan einzugeben und die Bereiche auszuwählen, die gescannt werden sollen.
5. Um die Scan-Optionen im Detail zu konfigurieren, wählen Sie den Reiter **Erweitert**.

   Sie können die Scan-Optionen einfach durch Einstellen der Scan-Tiefe festlegen. Schieben Sie den Regler dazu in die gewünschte Position.

   Sie können auch festlegen, dass der Computer heruntergefahren wird, wenn der Scan beendet und keine Bedrohung erkannt wurde. Bitte beachten Sie, dass dies das Standardverhalten bei jeder Ausführung dieser Aufgabe sein wird.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
7. Klicken Sie auf **Planen**, um eine Zeitplan für Ihre Scan-Aufgabe festzulegen.
8. Klicken Sie auf **Scan starten** und folgen Sie den Anweisungen des Assistenten für den Viren-Scan, um den Scan abzuschließen. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.
9. Bei Bedarf können Sie einen bereits durchgeführten benutzerdefinierten Scan einfach erneut ausführen, indem Sie auf den entsprechenden Eintrag in der Liste klicken.

12.4. Wie kann ich einen Ordner vom Scan ausnehmen?

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateiendungen vom Scan ausschließen.

Ausschlüsse sollten nur von Benutzern eingesetzt werden, die erfahren im Umgang mit Computern sind und nur in den folgenden Situationen:

- Sie haben einen großen Ordner mit Filmen und Musik auf Ihrem System gespeichert.
- Sie haben ein großes Archiv mit verschiedenen Daten auf Ihrem System gespeichert.
- Sie haben einen Ordner, in dem Sie verschiedene Software-Typen und Anwendungen zu Testzwecken installieren. Ein Scan des Ordners könnte zum Verlust einiger der Daten führen.

Um den Ordner des Ausschlussliste hinzuzufügen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Ausschlüsse** aus.
5. Vergewissern Sie sich, dass der Schalter für **Ausschlüsse für Dateien** auf EIN steht.
6. Klicken Sie auf den Link **Ausgeschlossene Dateien und Ordner**.
7. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
8. Klicken Sie auf **Durchsuchen**, wählen Sie den Ordner, der vom Scan ausgeschlossen werden soll, und klicken Sie auf **OK**.
9. Klicken Sie auf **Hinzufügen** und danach auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

12.5. Wie gehe ich vor, wenn Bitdefender eine saubere Datei als infiziert eingestuft hat?

Es können Situationen auftreten, in denen Bitdefender einwandfreie Dateien irrtümlicherweise als Bedrohung einstuft (Fehlalarm). Um diesen Fehler zu korrigieren, fügen Sie die Datei der Bitdefender-Ausschlussliste hinzu:

1. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Öffnen die den Bereich **Schutz**.
   c. Klicken Sie auf das Modul **Virenschutz**.
   d. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.
   e. Klicken Sie auf den Schalter, um **Zugriff-Scan** zu deaktivieren.

      Ein Fenster mit einer Warnung wird eingeblendet. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll. Zur Auswahl stehen 5, 15 oder 30 Minuten, eine Stunde, permanent oder bis zum nächsten Systemstart.
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 85).
3. Stellen Sie die Datei aus der Quarantäne wieder her:
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Öffnen die den Bereich **Schutz**.
   c. Klicken Sie auf das Modul **Virenschutz**.
   d. Wählen Sie im Fenster **Virenschutz** den Reiter **Quarantäne** aus.
   e. Wählen Sie die Datei aus und klicken Sie auf **Wiederherstellen**.
4. Fügen Sie die Datei zur Ausschlussliste hinzu. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie kann ich einen Ordner vom Scan ausnehmen?“* (S. 65).
5. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

6. Setzten Sie sich mit unseren Support-Mitarbeitern in Verbindung, damit wir die Erkennungssignatur entfernen können. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Hilfe anfordern“* (S. 238).

12.6. Wo sehe ich, welche Viren Bitdefender gefunden hat?

Nach jedem durchgeführten Scan wird ein Protokoll erstellt, in dem Bitdefender alle gefundenen Probleme aufzeichnet.

Der Bericht enthält detaillierte Informationen über den Scan-Vorgang, so wie Scan-Optionen, das Scan-Ziel, die gefundenen Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **Protokoll anzeigen** klicken.

Wenn Sie ein Scan-Protokoll lesen oder eine gefundene Infektion einsehen möchten, gehen Sie dazu wie folgt vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.
3. Wählen Sie im Fenster **Ereignisanzeige** **Virenschutz** aus dem entsprechenden Menü aus.

   Hier können Sie alle Malware-Scan-Ereignisse finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.
4. In der Ereignisliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
5. Um ein Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**. Das Scan-Protokoll wird in einem neuen Fenster geöffnet.

13. JUGENDSCHUTZ

13.1. Wie kann ich meine Kinder vor Bedrohungen aus dem Internet schützen?

Die Kindersicherung von Bitdefender ermöglicht es, den Zugriff auf das Internet und bestimmte Applikationen zu beschränken, um so zu verhindern, dass sich Ihre Kinder unangemessene Inhalte ansehen, wenn Sie nicht anwesend sind.

Um die Kindersicherung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Erstellen Sie eingeschränkte (Standard-) Windows-Benutzerkonten für Ihre Kinder. Für weitere Informationen lesen Sie bitte *„Wie lege ich Windows-Benutzerkonten an?“* (S. 71).
2. Stellen Sie sicher, dass Sie auf dem Computer eingeloggt sind, auf dem sich das Administrator-Benutzerkonto befindet. Nur Benutzer mit administrativen Rechten (Systemadministratoren) können auf die Kindersicherung zugreifen und sie konfigurieren.
3. Konfigurieren Sie die Kindersicherung für die Windows-Benutzerkonten Ihrer Kinder.
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Öffnen Sie den Bereich **Privatsphäre**.
   c. Wählen Sie im Modul **Kindersicherung Konfigurieren** aus.

      Stellen Sie sicher, dass Sie bei Ihrem MyBitdefender-Konto angemeldet sind.
   d. Das Kindersicherungs-Dashboard wird in einem neuen Fenster geöffnet. Hier können Sie die Einstellungen der Kindersicherung verändern.
   e. Klicken Sie im Menü links auf **Kind hinzufügen**.
   f. Geben Sie den Namen des Kindes im Reiter **Profil** ein. Durch die Angabe des Kindesalters werden automatisch für diese Altersstufe als geeignet eingeschätzte Einstellungen geladen. Diese Einstellungen basieren auf der Standard-Entwicklung von Kindern.

Über MyBitdefender können Sie von jedem beliebigen Computer oder Mobilgerät mit Internetzugang die Online-Aktivitäten Ihrer Kinder überwachen und die Einstellungen der Kindersicherung verändern.

Detaillierte Informationen zur Verwendung der Kindersicherung finden Sie im Kapitel *„Jugendschutz“* (S. 164).

13.2. Wie schränke ich den Internetzugang für mein Kind ein?

Wenn Sie die Kindersicherung eingerichtet haben, können Sie ganz leicht den Internetzugang auf bestimmte Zeiten begrenzen.

Mit der Bitdefender-Kindersicherung können Sie die Internetnutzung Ihrer Kinder steuern, selbst wenn Sie unterwegs sind.

So können Sie den Internetzugriff auf bestimmte Tageszeiten festlegen:

1. Öffnen Sie auf einem beliebigen Gerät mit Internetzugang einen Web-Browser.
2. Gehen Sie zu:https://my.bitdefender.com
3. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Ihrem Konto an.
4. Klicken Sie auf **Kindersicherung**, um das Dashboard zu öffnen.
5. Wählen Sie aus dem Menü links das Profil Ihres Kindes.
6. Klicken Sie im Bereich **Web** auf , um das Fenster **Web-Aktivität** zu öffnen.
7. Klicken Sie auf **Zeitplan**.
8. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff blockiert sein soll. Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren.
9. Klicken Sie auf den Button **Speichern**.



Beachten Sie

Bitdefender führt unabhängig davon, ob der Internetzugriff gesperrt ist, stündliche Updates durch.

13.3. Wie hindere ich mein Kind daran, eine bestimmte Website aufzurufen?

Mit der Bitdefender-Kindersicherung können Sie steuern, welche Inhalten sich Ihre Kinder im Internet ansehen, und gezielt den Zugriff auf bestimmte Websites blockieren, auch wenn Sie nicht zu Hause sind.

So können Sie den Zugriff auf eine bestimmte Website blockieren:

1. Öffnen Sie auf einem beliebigen Gerät mit Internetzugang einen Web-Browser.
2. Gehen Sie zu:https://my.bitdefender.com
3. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Ihrem Konto an.
4. Klicken Sie auf **Kindersicherung**, um das Dashboard zu öffnen.
5. Wählen Sie aus dem Menü links das Profil Ihres Kindes.
6. Klicken Sie im Bereich **Web** auf , um das Fenster **Web-Aktivität** zu öffnen.
7. Klicken Sie **Blacklist/Whitelist**.
8. Geben Sie die Website in das entsprechende Feld ein.
9. Klicken Sie auf **Blockieren**, um die Website zu der Liste hinzuzufügen.
10. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff erlaubt werden soll. Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren.

    Klicken Sie auf **OK**.
11. Wenn Sie sich später umentscheiden, wählen Sie einfach die Website aus und klicken Sie auf die entsprechende **Entfernen**-Schaltfläche.

13.4. Wie verhindere ich, dass mein Kind ein bestimmtes Spiel spielt?

Mit der Bitdefender-Kindersicherung können Sie steuern, auf welche Inhalte Ihre Kinder zugreifen können, wenn sie den Computer nutzen.

Mit der Bitdefender-Kindersicherung können Sie den Zugriff auf bestimmte Spiele und/oder Programme verhindern, auch wenn Sie nicht zu Hause sind.

Um den Zugriff auf ein Spiel zu blockieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie auf einem beliebigen Gerät mit Internetzugang einen Web-Browser.
2. Gehen Sie zu:https://my.bitdefender.com
3. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Ihrem Konto an.
4. Klicken Sie auf **Kindersicherung**, um das Dashboard zu öffnen.
5. Wählen Sie aus dem Menü links das Profil Ihres Kindes.
6. Klicken Sie Bereich **Anwendungen** auf , um das Fenster **Anwendungsaktivität** zu öffnen.
7. Klicken Sie auf **Blacklist**.
8. Geben Sie den Pfad zur ausführbaren Datei in das entsprechende Feld ein; Sie können ihn auch kopieren und hier einfügen.
9. Klicken Sie auf **Blockieren**, um die Anwendung zur **Blockierte Anwendungen** hinzuzufügen.
10. Wenn Sie sich später umentscheiden, klicken Sie auf die entsprechende **Zulassen**-Schaltfläche.

13.5. Wie lege ich Windows-Benutzerkonten an?

Ein Windows-Benutzerkonto ist ein eindeutiges Profil, zu dem alle Einstellungen, Zugriffsrechte und persönlichen Dateien des entsprechenden Benutzers gehören. Windows-Benutzerkonten lassen den Heim-PC-Administrator den Zugriff für jeden Benutzer kontrollieren.

Das Anlegen von Benutzerkonten ist dann sinnvoll, wenn sowohl Erwachsene als auch Kinder den PC benutzen - ein Elternteil kann für jedes Kind ein separates Benutzerkonto anlegen.

Wählen Sie Ihr Betriebssystem, um so herauszufinden, wie Sie Windows-Benutzerkonten erstellen können.

- **Windows XP:**
  1. Melden Sie sich an Ihrem Computer als Administrator ein.
  2. Klicken Sie auf "Start", klicken Sie auf "Systemsteuerung" und dann auf "Benutzerkonten".

3. Klicken Sie auf "Neues Benutzerkonto erstellen".
4. Geben Sie den Namen des Benutzers ein. Sie können den vollständigen Namen der Person, den Vornamen oder einen Spitznamen verwenden. Klicken Sie dann auf "Weiter".
5. Klicken Sie für diesen Benutzerkontentyp auf "Standard" und danach auf "Benutzerkonto erstellen". Begrenzte Benutzerkonten sind vor allem für Kinder geeignet, da keine systemübergreifenden Änderungen vorgenommen oder bestimmte Applikationen installiert werden können.
6. Ihr neues Benutzerkonto wird erstellt und dieses wird im Bildschirm "Benutzerkonten verwalten" aufgelistet.

- **Windows Vista oder Windows 7:**
  1. Melden Sie sich an Ihrem Computer als Administrator ein.
  2. Klicken Sie auf "Start", klicken Sie auf "Systemsteuerung" und dann auf "Benutzerkonten".
  3. Klicken Sie auf "Neues Benutzerkonto erstellen".
  4. Geben Sie den Namen des Benutzers ein. Sie können den vollständigen Namen der Person, den Vornamen oder einen Spitznamen verwenden. Klicken Sie dann auf "Weiter".
  5. Klicken Sie für diesen Benutzerkontentyp auf "Standard" und danach auf "Benutzerkonto erstellen". Begrenzte Benutzerkonten sind vor allem für Kinder geeignet, da keine systemübergreifenden Änderungen vorgenommen oder bestimmte Applikationen installiert werden können.
  6. Ihr neues Benutzerkonto wird erstellt und dieses wird im Bildschirm "Benutzerkonten verwalten" aufgelistet.

- **Windows 8:**
  1. Melden Sie sich an Ihrem Computer als Administrator ein.
  2. Bewegen Sie den Mauszeiger in den rechten oberen Bildschirmbereich, klicken Sie auf Einstellungen und PC-Einstellungen ändern.
  3. Klicken Sie im Menü links auf Benutzer und dann auf Benutzer hinzufügen.

     Sie können entweder ein Microsoft-Konto oder ein lokales Konto anlegen. Lesen Sie sich die Beschreibung für jeden Kontotyp durch und

befolgen Sie die Anweisungen auf dem Bildschirm, um ein neues Konto anzulegen.



Beachten Sie
Nun, da Sie neue Benutzerkonten hinzugefügt haben, können Sie für diese Passwörter vergeben.

13.6. Wie entferne ich das Profil für mein Kind?

Um ein bestehendes Profil für Ihr Kind zu entfernen, gehen Sie folgendermaßen vor:

1. Öffnen Sie auf einem beliebigen Gerät mit Internetzugang einen Web-Browser.
2. Gehen Sie zu: https://my.bitdefender.com.
3. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Ihrem Konto an.
4. Klicken Sie auf **Kindersicherung**, um das Dashboard zu öffnen.
5. Wählen Sie im Menü links das Profil aus, das Sie löschen möchten.
6. Klicken Sie auf **Konto-Einstellungen**.
7. Klicken Sie auf **Profil entfernen**.
8. Klicken Sie auf **OK**.

14. PRIVATSHPÄRESCHUTZ

14.1. Wie sichere ich meine Online-Transaktionen ab?

Um Ihre Online-Transaktionen wie Online-Banking noch sicherer zu machen, können Sie den Browser von Bitdefender verwenden.

Bitdefender Safepay™ ist ein abgesicherter Browser, der Ihre Kreditkartennummern, Kontonummern und andere sensible Daten, die Sie bei Online-Transaktionen eingeben, zuverlässig schützt.

So sichern Sie Ihre Online-Transaktionen ab:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie auf die **Safepay**-Schaltfläche auf der rechten Seite des Fensters.
3. Klicken Sie auf die Schaltfläche ▦, um die **Virtuelle Tastatur** aufzurufen.
4. Verwenden Sie die **Virtuelle Tastatur** immer dann, wenn Sie sensible Informationen wie Passwörter eingeben.

14.2. Wie schütze ich mein Facebook-Konto?

Safego ist eine Facebook-Anwendung, die von Bitdefender entwickelt wurde, um Ihr soziales Netzwerk zu schützen.

Ihre Aufgabe besteht darin, die Links, die Sie von Ihren Facebook-Freunden erhalten, zu scannen und die Privatsphäreeinstellungen Ihres Benutzerkontos zu überwachen.

Um auf Safego von Ihrem Bitdefender-Produkt aus zuzugreifen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras.**
3. Wählen Sie im Modul **Safego Facebook-Schutz aktivieren** aus.

   Sie werden zu Ihrem Konto weitergeleitet.
4. Nutzen Sie Ihre Facebook-Anmeldeinformationen, um sich mit der Safego-Anwendung zu verbinden.
5. Erlauben Sie Safego, auf Ihr Facebook-Konto zuzugreifen.

14.3. Wie schütze ich meine persönlichen Daten?

Um sicherzustellen, dass persönliche Daten Ihren Computer nicht ohne Ihre Zustimmung verlassen, müssen Sie angemessene Datenschutzregeln festlegen. Die Datenschutzregeln legen die Informationen fest, die blockiert werden sollen.

Um eine Datenschutzregel anzulegen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Privatsphäre**.
3. Klicken Sie auf das Modul **Datenschutz**.
4. Wenn der **Datenschutz** deaktiviert ist, aktivieren Sie ihn mithilfe des entsprechenden Schalters.
5. Wählen Sie die Option **Regel hinzufügen**, um den Assistenten für den Datenschutz zu starten.
6. Befolgen Sie die Anweisungen des Assistenten.

14.4. Wie lösche ich mit Bitdefender eine Datei unwiderruflich?

Wenn Sie eine Datei unwiderruflich von Ihrem System löschen möchten, müssen Sie die Datei physisch von Ihrer Festplatte entfernen.

Mit dem Bitdefender-Dateischredder können Sie über das Windows-Kontextmenü Dateien oder Ordner auf Ihrem Computer schnell und einfach schreddern. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, den Sie unwiderruflich löschen möchten, wählen Sie Bitdefender und anschließend **Dateischredder**.
2. Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **Ja**, um den Assistenten für den Dateischredder zu starten.
3. Bitte warten Sie, bis Bitdefender das Schreddern der Dateien abgeschlossen hat.
4. Die Ergebnisse werden angezeigt. Klicken Sie auf **Schließen**, um den Assistenten zu beenden.

15. PC-TUNING

15.1. Wie verbessere ich die Leistung meines Systems?

Die Systemleistung hängt nicht allein von der Hardware-Konfiguration wie Prozessorauslastung, Speichernutzung und Festplattenspeicher ab. Sie hängt zudem auch direkt von Ihrer Systemkonfiguration und Datenverwaltung ab.

Dies sind die Hauptaktionen, die Sie mit Bitdefender durchführen können, um die Systemgeschwindigkeit und -leistung zu verbessern.

- *„Defragmentieren Ihrer Festplatte“* (S. 76)
- *„Optimieren Sie Ihre Systemgeschwindigkeit mit nur einem Klick“* (S. 76)
- *„Scannen Sie Ihr System regelmäßig“* (S. 77)

15.1.1. Defragmentieren Ihrer Festplatte

Es empfiehlt sich, die Festplatte zu defragmentieren, um den Dateizugriff zu beschleunigen und die Gesamtleistung des Systems zu verbessern. Die Defragmentierung hilft Ihnen, die Dateifragmentierung zu vermindern und verbessert die Leistung Ihres Systems.

Um die Defragmentierung zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Wählen Sie im Bereich **PC-Tuning Defragmentierung** aus.
4. Befolgen Sie die Anweisungen des Assistenten.

Weitere Informationen zum Defragmentierungsmodul finden Sie im Kapitel *„Defragmentieren der Festplattenlaufwerke“* (S. 187).

15.1.2. Optimieren Sie Ihre Systemgeschwindigkeit mit nur einem Klick

Mit der Ein-Klick-Optimierung sparen Sie wertvolle Zeit bei der Verbesserung Ihrer Systemleistung, indem nicht mehr benötigte Dateien innerhalb kürzester Zeit gescannt, erkannt und bereinigt werden.

So können Sie die Ein-Klick-Optimierung starten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie im Modul **PC-Tuning** auf **Ein-Klick-Optimierung**.
4. Lassen Sie Bitdefender nach Dateien suchen, die gelöscht werden können, und klicken Sie auf **Optimieren**, um den Vorgang abzuschließen.

Noch schneller geht es mit einem Klick auf die **Optimieren**-Schaltfläche in der Bitdefender-Benutzeroberfläche.

Weitere Informationen, wie Sie die Systemgeschwindigkeit mit nur einem Klick verbessern können, erhalten Sie in Kapitel *„Optimierung der Systemgeschwindigkeit mit nur einem Klick“* (S. 183).

15.1.3. Scannen Sie Ihr System regelmäßig

Die Geschwindigkeit und das allgemeine Verhalten Ihres Systems kann auch durch Malware beeinträchtigt werden.

Stellen Sie sicher, dass Ihr System regelmäßig gescannt wird, mindestens einmal pro Woche.

Es empfiehlt sich, einen System-Scan durchzuführen, da so nach allen Malware-Typen gesucht wird, die die Sicherheit Ihres Systems bedrohen. Darüber hinaus werden auch die Inhalte von Archiven gescannt.

Um den System-Scan zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Wählen Sie im Modul **Virenschutz System-Scan** aus.
4. Befolgen Sie die Anweisungen des Assistenten.

15.2. Wie kann ich meine Systemstartzeit verbessern?

Nicht benötigte Anwendungen, die lästigerweise den Start des Systems verlangsamen, können mit der Systemstartoptimierung deaktiviert oder ihr Start verschoben werden, was Ihnen wertvolle Zeit spart.

So verwenden Sie die Systemstartoptimierung:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.

3. Klicken Sie im Modul **PC-Tuning** auf **Systemstartoptimierung**.
4. Wählen Sie die Anwendungen aus, die Sie beim Systemstart verzögern möchten.

Weitere Informationen, wie Sie die Startzeit Ihres PCs optimieren können, finden Sie in Kapitel *„Optimieren der Systemstartzeit“* (S. 184).

16. NÜTZLICHE INFORMATIONEN

16.1. Wie teste ich meine Virenschutzlösung?

Um die ordnungsgemäße Funktion Ihres Bitdefender-Produkts zu überprüfen, empfehlen wir den EICAR-Test.

Dabei testen Sie mithilfe der speziell für diesen Zweck entwickelten EICAR-Testdatei Ihren Virenschutz.

Um Ihre Virenschutzlösung zu testen, gehen Sie folgendermaßen vor:

1. Laden Sie die Testdatei von der offiziellen EICAR-Website unter http://www.eicar.org/ herunter.
2. Klicken Sie auf den Reiter **Anti-Malware Testfile**.
3. Klicken Sie im Menü links auf **Download**.
4. Klicken Sie unter **Download area using the standard protocol http** auf die **eicar.com**-Testdatei.
5. Sie werden informiert, dass die von Ihnen aufgerufene Seite die EICAR-Testdatei (kein Virus) enthält.

   Wenn Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken, beginnt der Download der Testdatei und ein Bitdefender-Fenster informiert Sie, dass ein Virus erkannt wurde.

   Klicken Sie auf **Mehr...** für weitere Informationen.

Falls Sie keine Bitdefender-Benachrichtigung erhalten, empfehlen wir Ihnen, sich wie in Kapitel *„Hilfe anfordern“* (S. 238) beschrieben an Bitdefender zu wenden.

16.2. Wie kann ich Bitdefender entfernen?

Um Ihr Bitdefender Internet Security 2015 zu entfernen, gehen Sie folgendermaßen vor:

- In **Windows XP**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme hinzufügen/entfernen**.
  2. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Entfernen**.
  3. Klicken Sie zum Fortfahren auf **Entfernen**.

4. Hier sind die folgenden Optionen verfügbar:
   - **Ich möchte es erneut installieren** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird nicht installiert.
   - **Ich möchte es dauerhaft entfernen** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird zum Schutz vor Malware auf Ihrem System installiert.

   Wählen Sie die gewünschte Option und klicken Sie auf **Weiter**.
5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- Für **Windows Vista** und **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.
  3. Klicken Sie zum Fortfahren auf **Entfernen**.
  4. Hier sind die folgenden Optionen verfügbar:
     - **Ich möchte es erneut installieren** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird nicht installiert.
     - **Ich möchte es dauerhaft entfernen** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird zum Schutz vor Malware auf Ihrem System installiert.

     Wählen Sie die gewünschte Option und klicken Sie auf **Weiter**.
  5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
- In **Windows 8**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.

4. Klicken Sie zum Fortfahren auf **Entfernen**.
5. Hier sind die folgenden Optionen verfügbar:
   - **Ich möchte es erneut installieren** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird nicht installiert.
   - **Ich möchte es dauerhaft entfernen** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird zum Schutz vor Malware auf Ihrem System installiert.

   Wählen Sie die gewünschte Option und klicken Sie auf **Weiter**.
6. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.



Beachten Sie

Der Bitdefender-60-Sekunden-Viren-Scanner ist eine kostenlose Anwendung, die auf In-the-Cloud-Scans setzt, um schädliche Programme und Bedrohungen in weniger als 60 Sekunden zu erkennen.

16.3. Wie kann ich mein System nach der Deinstallation von Bitdefender weiterhin schützen?

Während der Entfernung von Bitdefender Internet Security 2015 ist die Option **Ich möchte es dauerhaft entfernen** mit der Möglichkeit zur Installation des Bitdefender-60-Sekunden-Viren-Scanner verfügbar.

Der Bitdefender-60-Sekunden-Viren-Scanner ist eine kostenlose Anwendung, die auf In-the-Cloud-Scans setzt, um schädliche Programme und Bedrohungen in weniger als 60 Sekunden zu erkennen.

Sie können die Anwendung auch dann weiterhin nutzen, wenn Sie Bitdefender erneut installieren oder sich für ein anderes Virenschutzprogramm entscheiden.

Wenn Sie den Bitdefender-60-Sekunden-Viren-Scanner entfernen wollen, gehen Sie folgendermaßen vor:

- In **Windows XP**:

1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme hinzufügen/entfernen**.

2. Finden Sie den **Bitdefender-60-Sekunden-Viren-Scanner** und klicken Sie auf **Entfernen**.
3. Wählen Sie im nächsten Schritt **Deinstallieren** und warten Sie bis der Deinstallationsvorgang abgeschlossen ist.

- Für **Windows Vista** und **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Finden Sie den **Bitdefender-60-Sekunden-Viren-Scanner** und klicken Sie auf **Deinstallieren**.
  3. Wählen Sie im nächsten Schritt **Deinstallieren** und warten Sie bis der Deinstallationsvorgang abgeschlossen ist.
- In **Windows 8**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Wählen Sie den **Bitdefender-60-Sekunden-Viren-Scanner** aus und klicken Sie auf **Deinstallieren**.
  4. Wählen Sie im nächsten Schritt **Deinstallieren** und warten Sie bis der Deinstallationsvorgang abgeschlossen ist.

16.4. Wie fahre ich den Computer automatisch herunter, nachdem der Scan beendet wurde?

Bitdefender bietet unterschiedliche Scan-Aufgaben, mithilfe derer Sie sicherstellen können, dass Ihr System nicht mit Malware infiziert ist. Je nach Software- und Hardwarekonfiguration kann ein Scan des gesamten Systems längere Zeit in Anspruch nehmen.

Deshalb können Sie Bitdefender so konfigurieren, dass Bitdefender den Computer herunterfährt, sobald der Scan abgeschlossen ist.

Stellen Sie sich folgende Situation vor: Sie sind mit der Arbeit an Ihrem Computer fertig und möchten ins Bett gehen. Sie möchten aber nun noch Ihr System durch Bitdefender auf Malware prüfen lassen.

So können Sie einstellen, dass Bitdefender den Computer herunterfährt, sobald der Scan abgeschlossen ist:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Wählen Sie im Modul **Virenschutz Scans verwalten** aus.
4. Klicken Sie im Fenster **Scan-Aufgaben verwalten** auf **Neue benutzerdefinierte Aufgabe**, um einen Namen für den Scan einzugeben und die Bereiche auszuwählen, die gescannt werden sollen.
5. Um die Scan-Optionen im Detail zu konfigurieren, wählen Sie den Reiter **Erweitert**.
6. Markieren Sie die Option, dass der Computer heruntergefahren wird, wenn der Scan beendet und keine Bedrohung gefunden wurde.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
8. Klicken Sie **Prüfung Starten**.

Wenn keine Bedrohungen gefunden wurden, wird der Computer heruntergefahren.

Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen. Für weitere Informationen lesen Sie bitte *„Viren-Scan-Assistent“* (S. 103).

16.5. Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung?

Wenn Ihr Computer sich über einen Proxy-Server mit dem Internet verbindet, müssen Sie Bitdefender mit den Proxy-Einstellungen konfigurieren. Normalerweise findet und importiert Bitdefender automatisch die Proxy-Einstellungen Ihres Systems.



Wichtig

Internet-Verbindungen in Privathaushalten nutzen üblicherweise keine Proxy-Server. Als Faustregel gilt, dass Sie die Einstellungen der Proxy-Verbindung Ihrer Bitdefender-Anwendung prüfen und konfigurieren sollten, falls Updates nicht funktionieren. Wenn Bitdefender sich aktualisieren kann, dann ist es richtig konfiguriert, um eine Verbindung mit dem Internet aufzubauen.

Um die Proxy-Einstellungen zu verwalten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Erweitert** aus.
4. Klicken Sie auf den Schalter, um die Proxy-Nutzung einzuschalten.
5. Klicken Sie auf den Link **Proxyverwaltung**
6. Sie haben zwei Möglichkeiten, die Proxy-Einstellungen vorzunehmen:
   - **Proxy-Einstellungen aus Standard-Browser importieren** - Proxy-Einstellungen des aktuellen Benutzers, aus dem Standard-Browser importiert. Sollte ein Benutzername und Passwort nötig sein so geben Sie diesen in die dafür vorgesehenen Felder ein.

     Beachten Sie
     Bitdefender kann die Proxy-Einstellungen aus den gängigsten Browsern importieren, einschließlich der neuesten Versionen von Internet Explorer, Mozilla Firefox und Opera.

   - **Benutzerdefinierte Proxy-Einstellungen** - Proxy-Einstellungen, die Sie selbst konfigurieren können. Die folgenden Einstellungen müssen angegeben werden:
     - **Adresse** - Geben Sie die IP-Adresse des Proxy-Servers ein.
     - **Port** - Geben Sie den Port ein, über den Bitdefender die Verbindung zum Proxy-Server herstellt.
     - **Name** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
     - **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Bitdefender wird die verfügbaren Proxy-Einstellungen verwenden, bis die Lösung eine Verbindung mit dem Internet aufbauen kann.

16.6. Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert?

Um herauszufinden, ob auf Ihrem Computer ein 32- oder 64-Bit-Betriebssystem installiert ist, gehen Sie wie folgt vor:

- In **Windows XP**:
  1. Klicken Sie auf **Start**.
  2. Finden Sie **Arbeitsplatz** im Menü **Start**.
  3. Rechtsklicken Sie auf **Arbeitsplatz** und wählen Sie **Eigenschaften**.
  4. Wenn unter **System x64 Edition** aufgelistet ist, ist auf Ihrem System die 64-Bit-Version von Windows XP installiert.

     Wenn Sie den Punkt **x64 Edition** nicht finden, wird auf Ihrem Computer eine 32-Bit-Version von Windows XP ausgeführt.
- Für **Windows Vista** und **Windows 7**:
  1. Klicken Sie auf **Start**.
  2. Finden Sie **Computer** im **Start**-Menü.
  3. Rechtsklicken Sie auf **Arbeitsplatz** und wählen Sie **Eigenschaften**.
  4. Unter **System** können Sie die Systeminformationen einsehen.
- In **Windows 8**:
  1. Finden Sie auf der Windows-Startseite den Eintrag **Computer** (z.B. durch die Eingabe von "Computer" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Wählen Sie im Menü unten **Eigenschaften**.
  3. Unter **System** finden Sie Ihren Systemtyp.

16.7. Wie kann ich in Windows versteckte Objekte anzeigen?

Diese Schritte sind sinnvoll in den Fällen, in denen Sie es mit einer Malware-Situation zu tun haben und Sie infizierte Dateien, die eventuell verborgen sind, finden und entfernen müssen.

Gehen Sie folgendermaßen vor, um versteckte Objekte in Windows anzuzeigen:

1. Klicken Sie auf **Start** und öffnen Sie die **Systemsteuerung**.

   In **Windows 8**: Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
2. Klicken Sie auf **Ordneroptionen**.
3. Gehen Sie auf den Reiter **Ansicht**.
4. Wählen Sie **Inhalte des Systemverzeichnisses anzeigen** (nur für Windows XP).
5. Wählen Sie **Verborgene Dateien und Verzeichnisse anzeigen**.
6. Entfernen Sie den Haken bei **Erweiterungen bei bekannten Dateitypen ausblenden**.
7. Deaktivieren Sie **Geschützte Betriebssystemdateien verbergen**.
8. Klicken Sie auf **Anwenden** und dann auf **OK**.

16.8. Wie entferne ich andere Sicherheitslösungen?

Der Hauptgrund für den Einsatz einer Sicherheitslösung ist der Schutz und die Sicherheit Ihrer Daten. Aber was geschieht, wenn mehr als ein Sicherheitsprogramm auf demselben System läuft?

Wenn Sie mehr als eine Sicherheitslösung auf Ihrem Computer verwenden, wird dadurch das System instabil. Das Bitdefender Internet Security 2015-Installationsprogramm findet automatisch andere auf dem System installierte Sicherheits-Software und bietet an, diese zu deinstallieren.

Falls Sie weitere bereits auf dem PC installierte Sicherheits-Software nicht während der Installation entfernt haben, gehen Sie folgendermaßen vor:

- In **Windows XP**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme hinzufügen/entfernen**.
  2. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.

4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- Für **Windows Vista** und **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
- In **Windows 8**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  4. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

Wenn es Ihnen nicht gelingt, weitere auf Ihrem Rechner installierte Sicherheits-Software zu entfernen, laden Sie sich das Deinstallations-Tool von der Website des entsprechenden Herstellers herunter oder wenden Sie sich direkt an den Hersteller für eine Deinstallationsanleitung.

16.9. Wie nutze ich die Systemwiederherstellung unter Windows?

Wenn Sie den Computer nicht im Normalmodus starten können, starten Sie ihn im abgesicherten Modus und nutzen Sie die Systemwiederherstellung, um das System zu einem Zeitpunkt wiederherzustellen, an dem es ordnungsgemäß ausgeführt wurde.

Um eine Systemwiederherstellung durchzuführen, müssen Sie als Administrator bei Windows angemeldet sein.

Um die System-Wiederherstellung zu nutzen, gehen Sie folgendermaßen vor:

- In **Windows XP**:
  1. Starten Sie Windows im abgesicherten Modus.
  2. Folgen Sie diesem Pfad aus dem Windows-Startmenü heraus: **Alle Programme** → **Zubehör** → **Systemprogramme** → **Systemwiederherstellung**.
  3. Klicken Sie in dem Bildschirm **Willkommen zur Systemwiederherstellung** auf die Option **Meinen Computer zu einem früheren Zeitpunkt wiederherstellen** und danach auf Weiter.
  4. Wenn Sie den Anweisungen des Assistenten folgen, sollten Sie in der Lage sein, das System im Normalmodus zu starten.
- Für **Windows Vista** und **Windows 7**:
  1. Starten Sie Windows im abgesicherten Modus.
  2. Folgen Sie diesem Pfad aus dem Windows-Startmenü heraus: **Alle Programme** → **Zubehör** → **Systemprogramme** → **Systemwiederherstellung**.
  3. Wenn Sie den Anweisungen des Assistenten folgen, sollten Sie in der Lage sein, das System im Normalmodus zu starten.
- In **Windows 8**:
  1. Starten Sie Windows im abgesicherten Modus.
  2. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  3. Wählen Sie **Wiederherstellung** und danach **Systemwiederherstellung öffnen**.
  4. Wenn Sie den Anweisungen des Assistenten folgen, sollten Sie in der Lage sein, das System im Normalmodus zu starten.

16.10. Wie führe ich einen Neustart im abgesicherten Modus durch?

Der abgesicherte Modus ist ein diagnostischer Betriebsmodus, der hauptsächlich bei der Suche nach Fehlern zum Einsatz kommt, die den normalen Windows-Betrieb beeinträchtigen. Solche Probleme reichen von in Konflikt stehenden Treibern bis hin zu Viren, die Windows daran hindern, normal hochzufahren. Im abgesicherten Modus funktionieren nur einige wenige Anwendungen und Windows lädt nur die wichtigsten Treiber und ein Minimum an Betriebssystemkomponenten. Deshalb sind bei einer Verwendung von Windows im abgesicherten Modus die meisten Viren inaktiv und können einfach entfernt werden.

Start von Windows im abgesicherten Modus:

1. Starten Sie Ihren Computer neu.
2. Drücken Sie wiederholt die **F8**-Taste, bevor Windows startet, um so Zugriff auf das Boot-Menü zu erhalten.
3. Wählen Sie **Abgesicherter Modus** im Boot-Menü oder **Abgesicherter Modus mit Netzwerktreibern**, falls Sie Zugang zum Internet haben möchten.
4. Drücken Sie die **Eingabetaste** und warten Sie, während Windows im abgesicherten Modus startet.
5. Dieser Vorgang endet mit einer Bestätigungsbenachrichtigung. Klicken Sie zur Bestätigung auf **OK**.
6. Um Windows normal zu starten, starten Sie einfach Ihr System neu.

DIE SICHERHEITSELEMENTE IM DETAIL

17. VIRENSCHUTZ

Bitdefender schützt Sie vor allen Arten von Malware (Viren, Trojaner, Spyware, Rootkits etc.). Der Virenschutz, den Bitdefender bietet, lässt sich in zwei Kategorien einteilen:

- Zugriff-Scan - Verhindert, dass neue Malware-Bedrohungen auf Ihr System gelangen. Bitdefender wird z.B. ein Worddokument auf Malware scannen, wenn Sie es öffnen oder eine Email-Nachricht, wenn Sie diese empfangen.

  Der Zugriff-Scan stellt den Echtzeitschutz vor Malware sicher und ist damit ein grundlegender Bestandteil jedes Computer-Sicherheitsprogramms.

  ### Wichtig
  Um zu verhindern, dass Viren Ihren Computer infizieren, sollte der **Zugriff-Scan** immer aktiviert bleiben.

- On-demand Prüfung - erkennt und entfernt Malware die sich bereits auf dem System befindet. Hierbei handelt es sich um einen klassischen, durch den Benutzer gestarteten, Scan - Sie wählen das Laufwerk, Verzeichnis oder Datei, die Bitdefender scannen soll und Bitdefender scannt diese.

Bitdefender scannt automatisch alle Wechselmedien, die mit dem Computer verbunden sind, um einen sicheren Zugriff zu garantieren. Für weitere Informationen lesen Sie bitte *„Automatischer Scan von Wechselmedien“* (S. 108).

Erfahrene Benutzer können Scan-Ausschlüsse konfigurieren, wenn Sie nicht möchten, dass bestimmte Dateien oder Dateitypen gescannt werden. Für weitere Informationen lesen Sie bitte *„Konfiguration der Scan-Ausschlüsse“* (S. 110).

Wenn Bitdefender einen Virus oder andere Malware feststellt, versucht das Programm automatisch den Malware-Code der infizierten Datei zu entfernen und die Originaldatei wiederherzustellen. Diese Operation bezeichnet man als Desinfektion. Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Für weitere Informationen lesen Sie bitte *„Verwalten von Dateien in Quarantäne“* (S. 113).

Wenn Ihr Computer mit Malware infiziert ist, siehe *„Malware von Ihrem System entfernen“* (S. 225). Um Ihnen bei der Entfernung von Malware zu helfen, die nicht von innerhalb des Windows-Betriebssystems entfernt werden kann, stellt Bitdefender Ihnen einen Rettungsmodus zur Verfügung. Dabei handelt

es sich um eine vertrauenswürdige Umgebung, die speziell der Entfernung von Malware dient und es Ihnen ermöglicht, Ihren Computer unabhängig von Windows zu starten. Wenn der Computer im Rettungsmodus läuft, ist Windows-Malware inaktiv, wodurch sie sich leicht entfernen lässt.

Um Sie vor unbekannten schädlichen Anwendung zu schützen, nutzt Bitdefender mit Active Virus Control eine fortschrittliche heuristische Technologie, die alle Anwendungen auf Ihrem System ununterbrochen überwacht. Active Virus Control blockiert automatisch Anwendungen, die sich wie Malware verhalten, um zu verhindern, dass Sie Ihren Computer beschädigen. Mitunter werden auch legitime Anwendungen blockiert. In diesen Fällen können Sie Active Virus Control durch die Festlegung von Ausschlussregeln so konfigurieren, dass diese Anwendungen nicht noch einmal blockiert werden. Für weitere Informationen lesen Sie bitte das Kapitel *„Active Virus Control“* (S. 114).

17.1. Zugriff-Scans (Echtzeitschutz)

Bitdefender bietet durch die Prüfung aller aufgerufenen Dateien und E-Mail-Nachrichten durchgehenden Echtzeitschutz vor einer Vielzahl von Malware-Bedrohungen.

Die vorgegebenen Einstellungen zum Echtzeitschutz stellen einen guten Schutz gegen Malware bei nur minimaler Beeinträchtigung der Systemleistung sicher. Sie können die Einstellungen zum Echtzeitschutz einfach Ihren Bedürfnissen anpassen, indem Sie eine der vordefinierten Sicherheitsstufe wählen. Wenn Sie ein fortgeschrittener Benutzer sind, können Sie die Scan-Einstellungen auch selbst im Detail konfigurieren, indem Sie eine benutzerdefinierte Schutzstufe definieren.

17.1.1. Aktivieren / Deaktivieren des Echtzeitschutzes

Um den Echtzeitschutz vor Malware zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.

5. Klicken Sie auf den Schalter, um den Zugriff-Scan zu aktivieren oder deaktivieren.
6. Wenn Sie den Echtzeitschutz deaktivieren möchten erscheint ein Warnfenster. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll. Zur Auswahl stehen 5, 15 oder 30 Minuten, eine Stunde, permanent oder bis zum nächsten Systemstart. Der Echtzeitschutz wird automatisch nach Ablauf des festgelegten Zeitraums aktiviert.



Warnung

Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen den Echtzeitschutz so kurz wie möglich zu deaktivieren. Während der Echtzeitschutz deaktiviert ist sind Sie nicht vor Schädlingen geschützt.

17.1.2. Echtzeitschutz anpassen

Die Sicherheitsstufe des Echtzeitschutzes definiert die Scan-Einstellungen für den Echtzeitschutz. Sie können die Einstellungen zum Echtzeitschutz einfach Ihren Bedürfnissen anpassen, indem Sie eine der vordefinierten Sicherheitsstufe wählen.

Um die Echtzeitsicherheitsstufe anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.
5. Schieben Sie den Regler in die gewünschte Sicherheitsstufenposition. Verwenden Sie die Beschreibung auf der rechten Seite, um die Sicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

17.1.3. Einstellungen des Echtzeitschutzes konfigurieren

Erfahrene Benutzer können die Scan-Einstellungen von Bitdefender nutzen. Sie können die Einstellungen für den Echtzeitschutz im Detail konfigurieren, indem Sie eine benutzerdefinierte Sicherheitsstufe festlegen.

So können Sie die Einstellungen für den Echtzeitschutz anpassen:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.
5. Klicken Sie auf **Benutzerdefiniert**.
6. Konfigurieren Sie die Scan-Einstellungen nach Ihren Wünschen.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach. Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Scan-Optionen für aufgerufene Dateien.** Sie können Bitdefender so einstellen, dass Dateien oder Anwendungen (Programmdateien) nur bei Zugriff gescannt werden. Das Scannen aller Dateien bietet den besten Schutz, während das ausschließliche Scannen der Anwendungen nur für die Verbesserung der Systemleistung verwendet werden kann.

  Standardmäßig werden sowohl lokale Ordner als auch Netzwerkfreigaben durch Zugriff-Scans gescannt. Wenn Sie Ihre Systemleistung erhöhen möchten, können Sie Netzwerk-Ordner von Zugriff-Scans ausschließen.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Diese Kategorie beinhaltet die folgenden Dateierweiterungen:

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx;

smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Inhalt von Archiven scannen.** Das Scannen von Archiven ist ein langsamer und ressourcen-intensiver Vorgang, der aus diesem Grund nicht für den Echtzeitschutz empfohlen wird. Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit. Die Malware kann Ihr System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird.

  Wenn Sie sich entscheiden, diese Option zu nutzen, können Sie die maximale Größe der Archive angeben, die beim Zugriff-Scan durchsucht werden sollen. Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.

- **Scan-Optionen für E-Mail und Internet.** Um zu verhindern, dass Malware auf Ihren Computer geladen wird, scannt Bitdefender automatisch die folgenden Malware Einfalltore:
  - eingehende und ausgehende E-Mails
  - Internet-Datenverkehr

  Das Scannen des Web-Datenverkehrs kann Ihren Webbrowser geringfügig verlangsamen, dadurch können aber über das Internet übertragene Malware, einschließlich Drive-by-Downloads, blockiert werden.

  Sie können zur Steigerung der Systemleistung die Virenschutz-Scans für E-Mail und Internet deaktivieren, dies wird aber nicht empfohlen. Wenn Sie die entsprechenden Scan-Optionen deaktivieren, werden empfangene Emails und aus dem Internet geladene Dateien nicht gescannt. Dies bedeutet aber, dass infizierte Dateien auf Ihrem Computer gespeichert werden können. Dies ist keine bedeutende Bedrohung, da der Echtzeitschutz die Malware blockiert, wenn auf die infizierten Dateien zugegriffen wird (geöffnet, verschoben, kopiert oder ausgeführt).

- **Boot-Sektoren scannen.** Sie können Bitdefender einstellen, damit die Boot-Sektoren gescannt werden. Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.

- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Nach Keyloggern suchen.** Wählen Sie diese Option, um Ihr System auf Keylogger zu untersuchen. Keylogger zeichnen auf, was Sie auf Ihrer Tastatur tippen, und schicken dann via Internet Berichte an Hacker. Der Hacker kann über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und kann Sie zu seinem eigenen Profit verwenden.

Verfügbare Aktionen für gefundene Malware

Sie können einstellen, welche Aktionen der Echtzeit-Schutz ausführen soll.

Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.
5. Klicken Sie auf **Benutzerdefiniert**.
6. Konfigurieren Sie die Scan-Einstellungen nach Ihren Wünschen.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Der Echtzeit-Schutz in Bitdefender kann die folgenden Aktionen ausführen:

Aktionen ausführen

Bitdefender wird je nach Art der infizierten Datei die empfohlenen Aktionen ausführen:

- **Infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein. Bitdefender wird automatisch versuchen, den Malware-Code aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Diese Operation bezeichnet man als Desinfektion.

  Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem

Grund besteht kein Infektionsrisiko. Für weitere Informationen lesen Sie bitte *„Verwalten von Dateien in Quarantäne“* (S. 113).



Wichtig

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.

  Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

- **Archive mit infizierten Dateien.**
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch nicht infizierte Dateien enthält, wird Bitdefender versuchen, die infizierten Dateien zu löschen, vorausgesetzt, dass das Archiv mit den nicht infizierten Dateien wieder rekonstruiert werden kann. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Dateien in Quarantäne verschieben

Verschiebt die entdeckten Dateien in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Für weitere Informationen lesen Sie bitte *„Verwalten von Dateien in Quarantäne“* (S. 113).

Zugriff verweigern

Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.

17.1.4. Wiederherstellen der Standardeinstellungen

Die vorgegebenen Einstellungen zum Echtzeitschutz stellen einen guten Schutz gegen Malware bei nur minimaler Beeinträchtigung der Systemleistung sicher.

Um die Standardeinstellungen für den Echtzeitschutz wiederherzustellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.
5. Klicken Sie auf **Standard**.

17.2. On-Demand Prüfung

Die Aufgabe der Bitdefender-Software ist es sicherzustellen, dass es keine Viren in Ihrem System gibt. Dies wird erreicht, indem neue Viren ferngehalten und Ihre E-Mail-Nachrichten sowie alle heruntergeladenen oder auf Ihr System kopierten Dateien sorgfältig gescannt werden.

Es besteht aber die Gefahr, dass ein Virus bereits in Ihrem System ist, bevor Sie Bitdefender installieren. Deshalb sollten Sie Ihren Computer nach der Installation von Bitdefender auf residente Viren prüfen. Übrigens sollten Sie Ihren Computer auch in Zukunft häufig auf Viren prüfen.

Bedarf-Scans werden über Scan-Aufgaben ausgeführt. Die Scan-Aufgaben beinhalten die Scan-Optionen und die Objekte, die gescannt werden sollen. Sie können den Computer jederzeit scannen, indem Sie die Standard-Aufgaben oder Ihre eigenen Scan-Aufgaben (benutzerdefinierte Aufgaben) ausführen. Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.

17.2.1. Eine Datei oder einen Ordner nach Malware scannen

Wenn Sie den Verdacht hegen, dass Dateien und Verzeichnisse infiziert sein könnten, sollten Sie einen Scan durchführen. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, die/den Sie scannen möchten, wählen Sie **Bitdefender** und dann **Mit Bitdefender scannen**. Der

Viren-Scan-Assistent wird angezeigt. Er führt Sie durch den Scan-Vorgang. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

17.2.2. Durchführen von Quick Scans

Beim Quick Scan wird das sog In-the-Cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

Um einen Quick Scan auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Wählen Sie im Modul **Virenschutz Quick-Scan** aus.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

17.2.3. Durchführen von System-Scans

Der System-Scan scannt den gesamten Computer nach allen Malware-Arten wie Viren, Spyware, Adware, Rootkits usw.



Beachten Sie

Da ein **System-Scan** das gesamte System scannt, kann er eine Weile dauern. Es empfiehlt sich daher, diese Aufgabe durchzuführen, wenn Sie den Computer nicht benötigen.

Bevor Sie einen System-Scan ausführen, sollten Sie Folgendes beachten:

- Vergewissern Sie sich, dass die Malware-Signaturen von Bitdefender auf dem neuesten Stand sind. Ihren Computer unter Verwendung einer veralteten Signaturendatenbank zu prüfen, kann Bitdefender daran hindern neue Maleware, welche seit dem letzten Update gefunden wurde, zu

erkennen. Für weitere Informationen lesen Sie bitte *„Bitdefender auf dem neuesten Stand halten“* (S. 45).

- Schließen Sie alle geöffneten Programme.

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen. Für weitere Informationen lesen Sie bitte *„Benutzerdefinierte Scans durchführen“* (S. 100).

So führen Sie einen System-Scan durch:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Wählen Sie im Modul **Virenschutz System-Scan** aus.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

17.2.4. Benutzerdefinierte Scans durchführen

Um einen Malware-Scan im Detail zu konfigurieren und dann auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Wählen Sie im Modul **Virenschutz Scans verwalten** aus.
4. Klicken Sie auf **Neue benutzerdefinierte Aufgabe**. Klicken Sie auf den Reiter **Basic**, um einen Namen für den Scan einzugeben und die Bereiche auszuwählen, die gescannt werden sollen.
5. Um die Scan-Optionen im Detail zu konfigurieren, wählen Sie den Reiter **Erweitert**. Ein neues Fenster wird sich öffnen. Folgen Sie diesen Schritten:
    a. Sie können die Scan-Optionen einfach durch Einstellen der Scan-Tiefe festlegen. Schieben Sie den Regler dazu in die gewünschte Position. Die Beschreibung auf der rechten Seite der Skala helfen Ihnen, die Scan-Tiefe zu wählen, die für Ihre Bedürfnisse am besten geeignet ist.

Erfahrene Benutzer können die Scan-Einstellungen von Bitdefender nutzen. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Benutzerdefiniert**. Weitere Informationen zu den Optionen finden Sie am Ende dieses Kapitels.

b. Sie können auch folgende allgemeine Optionen konfigurieren:

- **Aufgabe mit niedriger Priorität ausführen .** Verringert die Priorität des Scan-Vorgangs. Dadurch können andere Programme schneller laufen, der Scan dauert aber länger.
- **Scan-Assistent in die Task-Leiste minimieren .** Minimiert das Scan-Fenster in die Task-Leiste Es kann durch einen Doppelklick auf das Bitdefender - Logo in der Symbolleiste wieder geöffnet werden.
- Wählen Sie die Aktion, die durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:

c. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

6. Klicken Sie auf den Schalter **Planen**, um eine Zeitplan für Ihre Scan-Aufgabe festzulegen. Wählen Sie eine der entsprechenden Optionen, um einen Zeitplan festzulegen:
   - Start bei Systemneustart
   - Einmal
   - Periodisch
7. Wählen Sie den Scan-Typ, den Sie über das Fenster **Scan-Aufgabe** ausführen möchten.
8. Klicken Sie auf **Scan starten** und folgen Sie den Anweisungen des Assistenten für den Viren-Scan, um den Scan abzuschließen. Abhängig von den Bereichen, die gescannt werden sollen, kann der Scan einige Zeit in Anspruch nehmen. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.
9. Bei Bedarf können Sie einen bereits durchgeführten benutzerdefinierten Scan einfach erneut ausführen, indem Sie auf den entsprechenden Eintrag in der Liste klicken.

Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach. Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Dateien prüfen.** Sie können Bitdefender so einstellen, dass alle Dateitypen oder nur Anwendungen (Programmdateien) gescannt werden. Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Diese Kategorie beinhaltet die folgenden Dateierweiterungen: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Scan-Optionen für Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit. Die Malware kann Ihr System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird. Wir empfehlen jedoch, diese Option zu nutzen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

  Beachten Sie

  Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Boot-Sektoren scannen.** Sie können Bitdefender einstellen, damit die Boot-Sektoren gescannt werden. Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher Ihres Systems laufen.
- **Registry scannen.** Wählen Sie diese Option, um die Registry-Schlüssel zu scannen. Die Windows-Registry ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.
- **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf Ihrem Computer gespeichert werden.
- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Kommerzielle Keylogger ignorieren.** Wählen Sie diese Option, wenn Sie auf Ihrem Computer eine kommerzielle Keylogger-Software nutzen. Kommerzielle Keylogger sind seriöse Programme zur Überwachung des Computers, deren Hauptfunktion es ist, alle Tastatureingaben aufzuzeichnen.
- **Nach Rootkits suchen.** Wählen Sie diese Option, um nach Rootkits und Objekten zu suchen, die mit dieser Art von Software versteckt werden.

17.2.5. Viren-Scan-Assistent

Wann immer Sie einen Bedarf-Scan starten (z. B. indem Sie mit der rechten Maustaste auf einen Ordner klicken, dann Bitdefender und anschließend **Mit Bitdefender scannen** wählen), wird der Bitdefender-Viren-Scan-Assistent eingeblendet. Folgen Sie den Anweisungen des Assistenten, um den Scan-Prozess abzuschließen.



Beachten Sie

Falls der Scan-Assistent nicht erscheint, ist der Scan möglicherweise konfiguriert, im Hintergrund zu laufen. Sehen Sie nach dem

Prüffortschritticon im Systemtray. Sie können dieses Objekt anklicken um das Scan-Fenster zu öffnen und so den Scan-Fortschritt zu sehen.

Schritt 1 - Führen Sie den Scan durch

Bitdefender startet den Scan der aus gewählten Dateien und Verzeichnisse. Sie erhalten Echtzeitinformationen über den Scan-Status sowie Scan-Statistiken (einschließlich der bisherigen Laufzeit, einer Einschätzung der verbleibenden Laufzeit und der Anzahl der erkannten Bedrohungen). Klicken Sie auf **Mehr anzeigen**, um weitere Details zu erhalten.

Bitte warten Sie, bis Bitdefender den Scan beendet hat. Der Scan-Vorgang kann, abhängig von der Größe Ihrer Festplatte, eine Weile dauern.

Einen Scan anhalten oder unterbrechen. Sie können den Scan-Vorgang jederzeit durch einen Klick auf **Stopp** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten. Um den Scan-Vorgang vorübergehend anzuhalten, klicken Sie einfach auf **Pause**. Um den Scan-Vorgang fortzusetzen klicken Sie auf **Fortsetzen** .

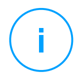
Passwortgeschützte Archive. Wird ein passwortgeschütztes Archiv gefunden, werden Sie, abhängig von den Scan-Einstellungen, um die Eingabe des Passwortes gebeten. Mit Passwort geschützte Archive können nicht gescannt werden, außer wenn Sie das Passwort angeben. Die folgenden Optionen sind verfügbar:

- **Passwort.** Wenn Sie möchten, dass Bitdefender Archive scannt, wählen Sie diese Option aus und geben das Passwort an. Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Nicht nach Passwort fragen; das Objekt beim Scan überspringen.** Wählen Sie diese Option um das Scannen diesen Archivs zu überspringen.
- **Alle passwortgeschützte Dateien überspringen ohne diese zu scannen.** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten. Bitdefender kann diese Dateien und Objekte nicht scannen, erstellt aber einen Eintrag im Scan-Protokoll.

Wählen Sie die gewünschte Option aus und klicken Sie auf **OK**, um den Scan fortzusetzen.

Schritt 2 - Wählen Sie entsprechende Aktionen aus

Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.



Beachten Sie

Wenn Sie einen Quick Scan oder einen vollständigen System-Scan durchführen, wird Bitdefender während des Scans automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Die infizierten Objekte werden in Gruppen angezeigt, je nach Malware, mit der sie infiziert sind. Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen. Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

Aktionen ausführen

Bitdefender wird je nach Art der infizierten Datei die empfohlenen Aktionen ausführen:

- **Infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein. Bitdefender wird automatisch versuchen, den Malware-Code aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Diese Operation bezeichnet man als Desinfektion.

  Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Für weitere Informationen lesen Sie bitte *„Verwalten von Dateien in Quarantäne“* (S. 113).



Wichtig

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.

  Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

- **Archive mit infizierten Dateien.**
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch nicht infizierte Dateien enthält, wird Bitdefender versuchen, die infizierten Dateien zu löschen, vorausgesetzt, dass das Archiv mit den nicht infizierten Dateien wieder rekonstruiert werden kann. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Löschen

Infizierte Dateien werden von der Festplatte entfernt.

Falls infizierte Dateien zusammen mit nicht infizierten Dateien in einem Archiv gespeichert sind, wird Bitdefender versuchen, die infizierten Dateien zu löschen und das Archiv mit den nicht infizierten Dateien zu rekonstruieren. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Keine Aktion ausführen

Es wird keine Aktion für die infizierte Dateien ausgeführt. Nachdem der Scan-Vorgang beendet wurde, können Sie das Scan-Protokoll öffnen um Informationen über diese Dateien anzuzeigen.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

Schritt 3 - Zusammenfassung

Wenn Bitdefender die Probleme gelöst hat, wird eine Zusammenfassung der Scan-Ergebnisse in einem neuen Fenster angezeigt. Falls Sie umfangreichere Informationen zum Scan-Prozess möchten, klicken Sie auf **Logdatei anzeigen**.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.



Wichtig

In den meisten Fällen desinfiziert Bitdefender erfolgreich die aufgespürten infizierten Dateien oder er isoliert die Infektion. Dennoch gibt es Probleme, die nicht automatisch gelöst werden können. Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Bereinigungsprozess abgeschlossen werden kann. Weitere Informationen und Anweisungen, wie Sie Malware manuell entfernen können, finden Sie unter *„Malware von Ihrem System entfernen“* (S. 225).

17.2.6. Scan-Protokolle lesen

Bei jedem Scan wird ein Scan-Protokoll erstellt, und Bitdefender zeichnet die gefundenen Probleme im Fenster Virenschutz auf. Der Bericht enthält detaillierte Informationen über den Scan-Vorgang, so wie Scan-Optionen, das Scan-Ziel, die gefundenen Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **Protokoll anzeigen** klicken.

Wenn Sie ein Scan-Protokoll lesen oder eine gefundene Infektion einsehen möchten, gehen Sie dazu wie folgt vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.
3. Wählen Sie im Fenster **Ereignisanzeige** **Virenschutz** aus dem entsprechenden Menü aus.

   Hier können Sie alle Malware-Scan-Ereignisse finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.

4. In der Ereignisliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
5. Um das Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**.

17.3. Automatischer Scan von Wechselmedien

Bitdefender erkennt automatisch, wenn Sie Wechselmedien mit Ihrem Computer verbinden und scannt diese im Hintergrund. Dies ist empfohlen um die Infizierung Ihres Systems durch Viren und andere Malware zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- USB-Speichergeräte, sowie Flashstifte und externe Festplatten
- verbundene (entfernte) Netzlaufwerke

Sie können den automatischen Scan der Speichermedien eigens für jede Kategorie konfigurieren. Der automatische Scan der abgebildeten Netzlaufwerke ist standardmäßig deaktiviert.

17.3.1. Wie funktioniert es?

Wenn ein Wechseldatenträger erkannt wird, beginnt Bitdefender diesen im Hintergrund nach Malware zu scannen (vorausgesetzt, dass der automatische Scan für diesen Gerätetyp aktiviert ist). Das Bitdefender-Scan-Symbol erscheint in der Task-Leiste. Sie können dieses Objekt anklicken um das Scan-Fenster zu öffnen und so den Scan-Fortschritt zu sehen.

Wenn der Auto-Pilot aktiviert ist, läuft der Scan ohne Ihr Zutun. Der Scan wird lediglich protokolliert und Sie können die dazugehörigen Informationen im Ereignis-Fenster abrufen.

Wenn der Autopilot deaktiviert ist:

1. Ein Pop-up-Fenster wird Sie darüber informieren, dass ein neues Gerät erkannt wurde und dass es derzeit gescannt wird.
2. In den meisten Fällen entfernt Bitdefender erkannte Malware automatisch oder isoliert infizierte Dateien in der Quarantäne. Sollte es nach dem Scan noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.



Beachten Sie

Beachten Sie, dass keine Aktion gegen infizierte oder verdächtige Dateien auf CDs/DVDs vorgenommen werden kann. Ähnlich können keine Aktionen gegen infizierte oder verdächtige Dateien auf Netzlaufwerken vorgenommen werden, wenn Sie nicht die entsprechenden Freigaben haben.

3. Sobald der Scan abgeschlossen ist, wird das Fenster mit den Scan-Ergebnissen angezeigt, um Sie darüber zu informieren, ob Sie die Dateien auf dem Wechselmedium gefahrlos aufrufen können.

Diese Informationen könnten sich als hilfreich erweisen:

- Bitte gehen Sie vorsichtig vor, wenn Sie eine CD oder DVD nutzen, die mit Malware infiziert ist, da diese nicht von dem Datenträger entfernt werden kann (diese Medien sind schreibgeschützt). Stellen Sie sicher, dass der Echtzeitschutz aktiviert ist, um zu verhindern, dass Malware auf Ihr System gelangt. Es empfiehlt sich, wichtige Daten vom Datenträger auf Ihr System zu kopieren und den Datenträger dann zu entsorgen.
- Es kann vorkommen, dass Bitdefender nicht in der Lage ist, Malware aus juristischen oder technischen Gründen aus bestimmten Dateien zu entfernen. Ein Beispiel hierfür sind Dateien, die mithilfe von proprietären Technologien archiviert wurden (der Grund dafür ist, dass das Archiv nicht korrekt wiederhergestellt werden kann).

  Um zu erfahren, wie Sie mit Malware umgehen sollen, lesen Sie bitte das Kapitel *„Malware von Ihrem System entfernen“* (S. 225).

17.3.2. Verwalten des Scans für Wechselmedien

Um die automatischen Scans für Wechselmedien zu verwalten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Ausschlüsse** aus.

Um den bestmöglichen Schutz zu garantieren, empfiehlt es sich, den automatischen Scan für alle Arten von Wechselmedien zu aktivieren.

Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert. Wenn infizierte Dateien erkannt werden, wird Bitdefender versuchen, diese

zu desinfizieren (d.h. den Malware zu entfernen) oder in die Quarantäne zu verschieben. Sollten beide Maßnahmen fehlschlagen, können Sie im Assistenten für den Virenschutz-Scan andere Aktionen für die infizierten Dateien festlegen. Die Prüfoptionen sind standartisiert, sie können daher nicht geändert werden.

17.4. Konfiguration der Scan-Ausschlüsse

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateiendungen vom Scan ausschließen. Diese Funktion soll verhindern, dass Sie bei Ihrer Arbeit gestört werden und kann zudem dabei helfen, die Systemleistung zu verbessern. Ausschlüsse sollten nur von Benutzern eingesetzt werden, die erfahren im Umgang mit Computern sind oder wenn dies von einem Bitdefender-Mitarbeiter empfohlen wurde.

Sie können Ausschlüsse so konfigurieren, dass sie für Zugriff-Scans, Bedarf-Scans oder beide Arten von Scans gelten. Die ausgenommenen Objekte werden nicht geprüft, egal ob der Zugriff von Ihnen oder von einem Programm erfolgt.



Beachten Sie

Ausschlüsse werden bei Kontext-Scans NICHT berücksichtigt. Kontextprüfung ist eine Art von On-Demand-Scan: Rechtsklicken Sie auf die zu scannende Datei oder das Verzeichnis und wählen Sie **Mit Bitdefender scannen**.

17.4.1. Dateien oder Ordner vom Scan ausschließen

Um bestimmte Dateien oder Ordner vom Scan auszuschließen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Ausschlüsse** aus.
5. Aktivieren Sie Scan-Ausschlüsse für Dateien durch Anklicken des entsprechenden Schalters.
6. Klicken Sie auf den Link **Ausgeschlossene Dateien und Ordner**. Es erscheint ein Fenster. Hier können Sie die Dateien und Ordner verwalten, die vom Scan ausgeschlossen sind.

7. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
   b. Klicken Sie auf **Durchsuchen**, wählen Sie die Datei oder den Ordner, der vom Scan ausgeschlossen werden soll, und klicken Sie auf **OK**. Alternativ können Sie den Datei- oder Ordnerpfad auch manuell (oder per Kopieren und Einfügen) in das Bearbeitungsfeld eingeben.
   c. Standardmäßig werden die ausgewählten Dateien oder Ordner sowohl vom Zugriff-Scan als auch vom Bedarf-Scan ausgeschlossen. Wählen Sie eine der anderen Optionen, um die Anwendung der Ausschlussregel anzupassen.
   d. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

17.4.2. Dateiendungen vom Scan ausschließen

Wenn Sie eine Dateiendung vom Scan ausschließen, wird Bitdefender Dateien mit dieser Endung unabhängig von ihrem Speicherort nicht mehr scannen. Der Ausschluss bezieht sich auch auf Dateien auf Wechselmedien, wie zum Beispiel CDs, DVDs, USB-Sticks oder Netzlaufwerke.



Wichtig
Lassen Sie Vorsichtig walten, wenn Sie Dateiendung vom Scan ausschließen, da solche Ausschlüsse Ihren Computer anfällig für Malware-Bedrohungen machen können.

Um Dateiendungen vom Scan auszuschließen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Ausschlüsse** aus.
5. Aktivieren Sie Scan-Ausschlüsse für Dateien durch Anklicken des entsprechenden Schalters.

6. Klicken Sie auf den Link **Ausgeschlossene Dateiendungen**. In dem Fenster, das jetzt angezeigt wird, können Sie die Dateiendungen verwalten, die vom Scan ausgenommen sind.
7. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
   b. Geben Sie die Dateiendungen ein, die vom Scan ausgeschlossen werden sollen. Trennen Sie einzelne Endungen mit einem Semikolon (;). Hier ein Beispiel:

      txt;avi;jpg
   c. Standardmäßig werden alle Dateien mit den festgelegten Dateiendungen sowohl vom Zugriff-Scan als auch vom Bedarf-Scan ausgeschlossen. Wählen Sie eine der anderen Optionen, um die Anwendung der Ausschlussregel anzupassen.
   d. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

17.4.3. Verwalten von Scan-Ausschlüssen

Werden die konfigurierten Scan-Ausschlüsse nicht mehr benötigt, empfehlen wir, diese zu löschen oder die Scan-Ausschlüsse zu deaktivieren.

Um die Scan-Ausschlüsse zu verwalten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Ausschlüsse** aus. Nutzen Sie die Optionen im Bereich **Dateien und Ordner**, um Scan-Ausschlüsse zu verwalten.
5. Um Scan-Ausschlüsse zu entfernen oder zu bearbeiten, klicken Sie auf einen der verfügbaren Links. Gehen Sie wie folgt vor:
   - Um einen Eintrag aus der Tabelle zu entfernen, markieren Sie diesen und klicken dann auf **Entfernen**.
   - Doppelklicken Sie auf einen Tabelleneintrag, um diesen zu bearbeiten(oder markieren Sie den Eintrag und klicken Sie dann auf

Bearbeiten.) Ein neues Fenster erscheint in welchem Sie die Erweiterung, den Pfad und den Prüftyp der Ausnahme festlegen können. Führen Sie die notwendigen Änderungen durch und klicken Sie dann auf **Ändern**.

6. Nutzen Sie den entsprechenden Schalter, um die Scan-Ausschlüsse zu deaktivieren.

17.5. Verwalten von Dateien in Quarantäne

Bitdefender isoliert mit Malware infizierte Dateien, die nicht desinfiziert werden können, sowie verdächtige Dateien in einem sicheren Bereich, der sogenannten Quarantäne. Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden.

Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

Zudem scannt Bitdefender nach jedem Update der Malware-Signaturen die Dateien der Quarantäne. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

Um Dateien in Quarantäne zu überprüfen und zu verwalten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Quarantäne** aus.
5. Dateien in Quarantäne werden von Bitdefender in Übereinstimmung mit den Standardeinstellungen für die Quarantäne automatisch verwaltet. Sie können die Quarantäneeinstellungen an Ihre Anforderungen anpassen, dies wird aber nicht empfohlen.

   Quarantäne nach Signaturupdate erneut scannen

   Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch nach jedem Update der Virendefinitionen zu scannen. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

Verdächtige Dateien in Quarantäne zur weiteren Analyse übermitteln
Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch an das Bitdefender-Labor zu schicken. Die Beispieldateien werden dann von den Bitdefender-Malware-Forschern analysiert. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

Inhalte löschen, die älter als {30} Tage sind
Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht. Wenn Sie diesen Zeitraum verändern möchten, geben Sie einen neuen Wert in das entsprechende Feld ein. Um das automatische Löschen von alten Dateien in Quarantäne zu deaktivieren, geben Sie eine 0 ein.

6. Um eine Quarantäne-Datei zu löschen, markieren Sie diese und klicken dann auf den Button **Löschen**. Wenn Sie eine Quarantäne-Datei am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **Wiederherstellen**.

17.6. Active Virus Control

Active Virus Control von Bitdefender ist eine innovative und vorbeugende Erkennungstechnologie, die hoch entwickelte heuristische Methoden nutzt, um mögliche neue Bedrohungen in Echtzeit zu erkennen.

Die Active Virus Control überwacht kontinuierlich die auf Ihrem Computer laufenden Applikationen auf Malware-ähnliche Aktionen. Jede dieser Aktionen wird eingestuft, für jeden Prozess wird weiterhin eine Allgemeineinstufung erstellt. Wenn diese Gesamteinstufung für einen Prozess einen bestimmten Grenzwert überschreitet, wird der entsprechende Prozess als schädlich eingestuft und automatisch blockiert.

Wenn der Auto-Pilot deaktiviert ist, wird Sie ein Pop-up-Fenster über die blockierte Anwendung informieren. Andernfalls wird die Anwendung ohne Benachrichtigung blockiert. Im Ereignis-Fenster können Sie überprüfen, welche Anwendungen von Active Virus Control erkannt wurden.

17.6.1. Überprüfen erkannter Anwendungen

Um die Anwendungen zu überprüfen, die von Active Virus Control erkannt wurden, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.

2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.
3. Wählen Sie im Fenster **Ereignisanzeige Virenschutz** aus dem entsprechenden Menü aus.
4. Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
5. Wenn Sie der Anwendung vertrauen, klicken Sie auf **Zulassen und überwachen**, um Active Virus Control so zu konfigurieren, dass sie nicht mehr blockiert wird. Active Virus Control wird ausgeschlossene Anwendungen auch weiterhin überwachen. Wird bei einer ausgeschlossenen Anwendung verdächtiges Verhalten erkannt, wird das Ereignis lediglich protokolliert und als Erkennungsfehler in die Bitdefender-Cloud gemeldet.

17.6.2. Aktivieren / Deaktivieren von Active Virus Control

Um Active Virus Control zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.
5. Klicken Sie auf den Schalter, um Active Virus Control zu aktivieren oder deaktivieren.

17.6.3. Active-Virus-Control anpassen

Sollte Ihnen auffallen, das Active Virus Control häufig ungefährliche Anwendung erkennt, sollten Sie eine tolerantere Sicherheitsstufe auswählen.

Um den Schutz durch Active Virus Control anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.
5. Stellen Sie sicher, dass Active Virus Control aktiviert ist.

6. Schieben Sie den Regler in die gewünschte Sicherheitsstufenposition. Verwenden Sie die Beschreibung auf der rechten Seite, um die Sicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.



Beachten Sie

Je höher Sie die Sicherheitsstufe einstellen, desto weniger Anzeichen verdächtiger Aktivitäten braucht Active Virus Control, um einen Prozess zu melden. Dadurch steigt die Zahl der gemeldeten Anwendungen, aber auch die Wahrscheinlichkeit von Fehlalarmen (ungefährlichen Anwendungen, die dennoch als schädlich eingestuft wurden).

17.6.4. Verwalten von ausgeschlossenen Prozessen

Sie können Ausschlussregeln für vertrauenswürdige Anwendungen festlegen, damit Active Virus Control diese nicht blockiert, wenn sie sich wie Malware verhalten. Active Virus Control wird ausgeschlossene Anwendungen auch weiterhin überwachen. Wird bei einer ausgeschlossenen Anwendung verdächtiges Verhalten erkannt, wird das Ereignis lediglich protokolliert und als Erkennungsfehler in die Bitdefender-Cloud gemeldet.

Um die Prozesse zu verwalten, die von Active Virus Control ausgeschlossen sind, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Ausschlüsse** aus.
5. Klicken Sie auf den Link **Ausgeschlossene Prozesse**. Ein Fenster wird angezeigt. Hier können Sie die Prozesse verwalten, die von Active Virus Control ausgeschlossen sind.



Beachten Sie

Ausschlussregeln für Prozesse gelten auch für die Angriffserkennung.

6. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:

   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.

b. Klicken Sie auf **Durchsuchen**, wählen Sie die Anwendung, die ausgeschlossen werden soll und klicken Sie dann auf **OK**.

c. Lassen Sie die **Zulassen**-Option aktiviert, um zu verhindern, dass Active Virus Control die Anwendung blockiert.

d. Klicken Sie auf **Hinzufügen**.

7. Um Ausschlüsse zu entfernen oder zu bearbeiten, gehen Sie folgendermaßen vor:

   - Um ein Objekt aus der Liste zu entfernen markieren Sie es und klicken Sie dann auf die **Entfernen**-Schaltfläche
   - Doppelklicken Sie auf einen Tabelleneintrag, um diesen zu bearbeiten (oder markieren Sie den Eintrag und klicken Sie dann auf **Ändern**.) Führen Sie die notwendigen Änderungen durch und klicken Sie dann auf **Ändern**.

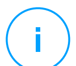
8. Speichern Sie die Änderungen, und schließen Sie das Fenster.

18. ANTISPAM

Spam ist ein Begriff, den man für unaufgeforderte Emails verwendet. Spam ist ein wachsendes Problem für Heimanwender wie auch für Organisationen. Sie wollen wahrscheinlich nicht, dass Ihre Kinder die meisten dieser Spam-Mails mit häufig pornographischem Inhalt lesen oder dass Sie deswegen sogar in Unannehmlichkeiten geraten. Spam wird immer mehr zum Ärgernis. Daher ist es das Beste, diese Mails gar nicht mehr zu erhalten.

Bitdefender Antispam greift auf außergewöhnliche technologische Innovationen und Standard-Antispam-Filter zurück, um Spams auszusortieren, bevor dieser im Posteingang landen. Für weitere Informationen lesen Sie bitte *„Wie funktioniert der Spam-Schutz?“* (S. 119).

Der Bitdefender Antispam-Schutz ist nur für Email Clients verfügbar, die Emails über das POP3-Protokoll zu empfangen. POP3 ist eines der am meisten benutzten Protokolle für das Downloaden der E-Mail-Nachrichten vom Mail-Server.



Beachten Sie

Bitdefender bietet keinen Antispam-Schutz für Email-Konten, auf die Sie über einen web-basierten Email-Service zugreifen.

Von Bitdefender aufgespürte Spams werden in der Betreffzeile mit dem [spam]-Marker gekennzeichnet. Bitdefender legt Spam-Nachrichten automatisch in einem festgelegten Verzeichnis ab, wie folgt:

- In Microsoft Outlook, Spams werden verschoben in den **Spam** Ordner, zu finden unter **gelöschte Objekte**. Das **Spam**-Verzeichnis wurde während der Installation von Bitdefender erstellt.
- In Outlook Express und Windows Mail, werden Spams direkt in **gelöschte Objekte** verschoben.
- Im Mozilla Thunderbird, werden Spams in den **Spam** Ordner verschoben, der unter **Trash** Ordner zu finden ist. Das **Spam**-Verzeichnis wurde während der Installation von Bitdefender erstellt.

Falls Sie andere E-Mail-Clients verwenden, müssen Sie eine Regel erstellen, um Nachrichten, die von Bitdefender als [spam] markiert wurden, in einen eigens erstellten Quarantäne-Ordner zu verschieben.

18.1. Wie funktioniert der Spam-Schutz?

18.1.1. AntiSpam Filter

Die Bitdefender-Spamschutz-Engine nutzt Cloud-Schutz und eine Reihe verschiedener Filter, um Ihren Posteingang frei von SPAM zu halten, so zum Beispiel die Freundesliste, Spammer-Liste und Zeichensatz-Filter..

Freundesliste/ Spammer-Liste

Viele Menschen kommunizieren normalerweise mit einer bestimmten Gruppe von Menschen oder aber erhalten Nachrichten von Firmen oder Organisationen mit derselben Domain. Wird eine **Freunde-/Spammerliste** geführt, so können Sie festlegen, welche Emails Sie erhalten wollen (die von Freunden) und welche Sie nicht erhalten möchten (die von Spammern).



Beachten Sie

Wir empfehlen, dass Sie die Namen Ihrer Freunde und deren Email-Adressen der **Freundeliste** hinzufügen, damit sichergestellt ist, dass nur solche Emails an Sie weitergeleitet werden. Bitdefenderblockiert keine Nachrichten dieser Absender. Somit stellt die Liste der Freunde sicher, dass alle legitimen Nachrichten auch ankommen.

Zeichensatz-Filter

Viele der Spam-Mails sind in Kyrillisch und/oder Asiatisch geschrieben. Der Zeichensatz-Filter erkennt diese Art von Nachrichten und markiert sie als SPAM.

18.1.2. Spam-Schutz

Die Bitdefender Antispam Engine kombiniert alle Antispam-Filter um festzustellen, ob eine bestimmte Email in den **Posteingang** gelangen sollte, oder nicht.

Jede E-Mail, die aus dem Internet kommt, wird zuerst mit den Filtern Freundesliste/Spammerliste überprüft. Falls die Adresse des Absenders in der Freundesliste gefunden wird, wird diese E-Mail direkt in Ihren **Posteingang** verschoben.

Wenn nicht, überprüft der Filter Spammerliste, ob der Absender der E-Mail auf der Liste der Spammer steht. Falls dem so ist, wird die E-Mail als Spam markiert und in den **Spam**-Ordner verschoben.

Der Zeichensatz-Filter überprüft, ob die E-Mail in kyrillischen oder asiatischen Zeichen geschrieben wurde. Falls dem so ist, wird die E-Mail als Spam markiert und in den **Spam**-Ordner verschoben.



Beachten Sie

Wenn die email in der Betreffzeile als „ausdrücklich sexuell" gekennzeichnet wurde, stuft Bitdefender die Email als Spam ein.

18.1.3. Unterstützte E-Mail-Clients und Protokolle

Der Antispam-Schutz steht für alle POP3/SMTP E-Mail-Clients zur Verfügung. Die Bitdefender Antispam-Toolbar wird integriert in:

- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express und Windows Mail (auf 32-Bit-Systemen)
- Mozilla Thunderbird 3.0.4

18.2. Aktivieren / Deaktivieren des Spam-Schutzes

Der Spam-Schutz ist standardmäßig aktiviert.

Um das Spam-Schutz-Modul zu deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Spam-Schutz**.
4. Klicken Sie im Fenster **Spam-Schutz** auf den Schalter, um den **Spam-Schutz** zu aktivieren oder deaktivieren.

18.3. Verwenden der Spam-Schutz-Symbolleiste in Ihrem Mail-Client-Fenster

Im oberen Teil Ihres Mail Client Fensters können Sie die Antispamleiste sehen. Die Antispamleiste hilft Ihnen beim Verwalten des Antispamschutzes direkt vom E-Mail Client aus. Sie können Bitdefender ganz einfach korrigieren, falls eine reguläre Mail als Spam markiert wurde.



Wichtig

Bitdefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste. Um die komplette Liste der

unterstützen E-Mail Clients, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle“* (S. 120).

Unten stehend finden Sie eine Beschreibung aller Buttons der Bitdefender-Symbolleiste:

Ist Spam - Gibt an, dass es sich bei der ausgewählten E-Mail um Spam handelt. Die E-Mail wird sofort in den **Spam**-Ordner verschoben. Wenn die Cloud-Dienste für den Spam-Schutz aktiviert sind, wird die Nachricht zur weiteren Analyse in die Bitdefender-Cloud geschickt.

Kein Spam - Zeigt an, dass es sich bei der angezeigten E-Mail nicht um Spam handelt und dass Bitdefender sie nicht als solche hätte kennzeichnen sollen. Die E-Mail wird aus dem **Spam** Ordner ins **Inbox** Ordner verschoben. Wenn die Cloud-Dienste für den Spam-Schutz aktiviert sind, wird die Nachricht zur weiteren Analyse in die Bitdefender-Cloud geschickt.



Wichtig

Der Button **Kein Spam** wird aktiv, wenn Sie eine Nachricht als Spam markiert haben von Bitdefender (normalerweise werden diese Nachrichten in den **Spam**-Verzeichnis verschoben).

Neuer Spammer - fügt den Absender der ausgewählten E-Mail zur Liste der Spammer hinzu. Klicken Sie zur Bestätigung **OK**. Die E-Mail-Nachrichten, die von den Adressen aus der Spammerliste empfangen werden, werden automatisch markiert als [spam].

Neuer Freund - fügt den Sender der ausgewählten E-Mail der Liste der Freunde hinzu. Klicken Sie zur Bestätigung **OK**. Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.

Spammer - Öffnen Sie **Spammerliste**. Sie enthält alle E-Mail-Adressen, von denen Sie keine Nachricht erhalten wollen, gleichwelchen Inhalts. Für weitere Informationen lesen Sie bitte *„Konfigurieren der Spammerliste“* (S. 124).

Freunde - Öffnen Sie **Freundenliste**. Sie enthält alle E-Mail-Adressen, von denen Sie immer Nachrichten erhalten wollen, gleichwelchen Inhalts. Für weitere Informationen lesen Sie bitte *„Konfigurieren der Freundesliste“* (S. 123).

Einstellungen - Öffnet eine Fenster, in dem Sie die Spam-Filter und die Einstellungen für die Symbolleiste konfigurieren können.

18.3.1. Anzeigen von Erkennungsfehlern

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie den Spam-Filter einfach korrigieren (indem Sie angeben, welche E-Mails nicht

als [spam] hätten markiert werden sollen). Dadurch wird die Effizienz des Spam-Filters verbessert. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Wählen Sie die Nachricht, die von Bitdefender fälschlicherweise als [spam] markiert wurde, aus.
4. Klicken Sie auf **Neuer Freund** in der Bitdefender-Spam-Schutz-Symbolleiste. Klicken Sie zur Bestätigung **OK**. Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.
5. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Kein Spam**. Die E-Mail wird in den Posteingangsordner verschoben.

18.3.2. Hinweisen auf unerkannte Spam-Nachrichten

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie einfach angeben, welche E-Mails als Spam hätten markiert werden sollen. Dadurch wird die Effizienz des Spam-Filters verbessert. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Begeben Sie sich zum Inbox Ordner.
3. Wählen Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Ist Spam**. Sie werden dann sofort als [spam] markiert und in den Junk-Ordner verschoben.

18.3.3. Konfigurieren der Symbolleisteneinstellungen

Um die Einstellungen für die Spam-Schutz-Symbolleiste in Ihrem E-Mail-Client zu konfigurieren, klicken Sie in der Symbolleiste auf die Schaltfläche **Einstellungen** und danach auf den Reiter **Symbolleisteneinstellungen**.

Dabei haben Sie die folgenden Möglichkeiten:

- **Nachricht verschieben nach Gelöschte Objekte** (nur für Microsoft Outlook Express / Windows Mail)



Beachten Sie
In Microsoft Outlook / Mozilla Thunderbird werden erkannte Spam-Nachrichten automatisch in einen Spam-Ordner verschoben, der sich wiederum im Ordner für gelöschte Elemente / Papierkorb befindet.

- **Markieren Sie Spam-E-Mail Nachrichten als 'gelesen'** - Markiert die Spam-Nachrichten automatisch als gelesen, so dass sie nicht stören wenn Sie ankommen.
- Sie können festlegen, ob Bestätigungsfenster angezeigt werden sollen, wenn Sie in der Spam-Schutz-Symbolleiste die Schaltflächen **Neuer Spammer** und **Neuer Freund** anklicken.

  Bestätigungsfenster verhindern, dass Sie die Absender von E-Mail-Nachrichten versehentlich zu Ihrer Freundes- bzw. Spam-Liste hinzufügen.

18.4. Konfigurieren der Freundesliste

Die **Liste der Freunde** ist eine Liste, die alle E-Mail-Adressen enthält, von denen Sie immer Nachrichten erhalten möchten, egal, welchen Inhalt sie haben. Nachrichten Ihrer Freunde werden nicht als Spam markiert, auch wenn der Inhalt dem von Spam ähnlich sein sollte.



Beachten Sie
Jede Mail von einer Adresse Ihrer **Freundesliste** wird automatisch in Ihren Posteingang verschoben.

Konfigurierung und Verwaltung der Freundeliste:

- Wenn Sie Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird nutzen, klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste auf die Schaltfläche **Freunde**.
- Alternativ folgen Sie diesen drei Schritten:
  1. Öffnen Sie das Bitdefender-Fenster.
  2. Öffnen die den Bereich **Schutz**.
  3. Wählen Sie im Modul **Spam-Schutz Freunde verwalten** aus.

Um eine E-Mail-Adresse hinzuzufügen, wählen Sie die Option **E-Mail-Adresse** und klicken Sie dann auf **Hinzufügen**. Syntax: name@domain.com.

Um alle E-Mail-Adressen einer bestimmten Domain hinzuzufügen, wählen Sie die Option **Domain-Name**, geben Sie den Domain-Namen ein und klicken Sie auf **Hinzufügen**. Syntax:

- @domain.com, *domain.com und domain.com - alle eingehenden Mails von domain.com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- *domain* - alle eingehenden Mails von domain werden ohne Überprüfung Ihres Inhaltes in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- *com - alle Mails mit der Endung com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;

Wir empfehlen, keine kompletten Domains hinzuzufügen, in einigen Situationen kann dies jedoch sinnvoll sein. Sie können beispielsweise die Email-Domain der Firma, für die Sie arbeiten, oder die von vertrauenswürdigen Partnern hinzufügen.

Um ein Objekt aus der Liste zu löschen, klicken Sie auf den entsprechenden **Entfernen**-Link. Klicken Sie auf **Liste leeren**, um alle Einträge aus der Liste zu löschen.

Sie können die Liste der Freunde speichern, so das diese auf einen anderen Rechner oder nach einer neuinstallation benutzt werden kann. Um die Freundesliste zu speichern klicken Sie auf **Speichern** und speichern sie diese an den gewünschten Ort. Die Datei wird .bwl als Erweiterung haben.

Um eine zuvor gespeicherte Freundesliste zu laden, klicken Sie **Laden** und öffnen die entsprechende .bwl Datei. Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Liste überschreiben**.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

18.5. Konfigurieren der Spammerliste

Liste der Spammer - Liste die alle E-Mail-Adressen enthält, von denen Sie keine Nachrichten erhalten wollen, gleich welchen Inhalts. Jede Mail von einer Adresse Ihrer **Spammerliste** wird automatisch in Ihren Papierkorb verschoben.

Konfigurierung und Verwaltung der Spammer-Liste:

- Wenn Sie Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird nutzen, klicken Sie in der in den Mail-Client integrierten Bitdefender-Spam-Schutz-Symbolleiste auf die Schaltfläche **Spammer**.
- Alternativ folgen Sie diesen drei Schritten:
  1. Öffnen Sie das Bitdefender-Fenster.
  2. Öffnen die den Bereich **Schutz**.
  3. Wählen Sie im Modul **Spam-Schutz Spammer verwalten** aus.

Um eine E-Mail-Adresse hinzuzufügen, wählen Sie die Option **E-Mail-Adresse** und klicken Sie dann auf **Hinzufügen**. Syntax: name@domain.com.

Um alle E-Mail-Adressen einer bestimmten Domain hinzuzufügen, wählen Sie die Option **Domain-Name**, geben Sie den Domain-Namen ein und klicken Sie auf **Hinzufügen**. Syntax:

- @domain.com, *domain.com und domain.com - alle eingehenden Mails von domain.com werden als Spam markiert;
- *domain* - alle eingehenden Mails von domain (egal welcher Endung) werden als Spam markiert;
- *com - alle Mails mit dieser Endung com werden als Spam markiert.

Wir empfehlen, keine kompletten Domains hinzuzufügen, in einigen Situationen kann dies jedoch sinnvoll sein.



Warnung

Fügen Sie keine legitimen Web-Mail-Anbieter (wie z. B. Gmail, GMX oder Web.de) zur Spammer-Liste hinzu. Sonst werden sämtliche E-Mails aller Benutzer solcher Anbieter als Spam eingestuft. z.B: wenn Sie yahoo.com zu Spammerliste hinzufügen, werden alle E-Mails die von yahoo.com Adressen kommen, als [spam] markiert.

Um ein Objekt aus der Liste zu löschen, klicken Sie auf den entsprechenden **Entfernen**-Link. Klicken Sie auf **Liste leeren**, um alle Einträge aus der Liste zu löschen.

Sie können die Spammer Liste in eine Datei sichern, damit Sie sie nach einer Neuinstallation oder auf einem anderen Computer nutzen können. Um die Spammerliste zu speichern klicken Sie auf **Speichern** und speichern sie diese an den gewünschten Ort. Die Datei wird .bwl als Erweiterung haben.

Um eine zuvor gespeicherte Spammerliste zu laden, klicken Sie **Laden** und öffnen die entsprechende .bwl Datei. Um den Inhalt einer aktuellen Liste

zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Liste überschreiben**.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

18.6. Konfigurieren der lokalen Spam-Schutz-Filter

Wie in *„Wie funktioniert der Spam-Schutz?“* (S. 119) beschrieben, nutzt Bitdefender eine Kombination aus unterschiedlichen Spam-Filtern, um Spam zu identifizieren. Die Spam-Filter sind für effizienten Schutz vorkonfiguriert.



Wichtig

Abhängig davon, ob Sie legitime Emails mit asiatischen oder kyrillischen Zeichen erhalten, aktivieren oder deaktivieren Sie die Einstellung, die solche Emails automatisch abblockt. Die entsprechende Einstellung ist in den lokalisierten Programmversion deaktiviert, die solche Zeichensätze verwendetn(wie z. B. in der russischen oder chinesischen Programmversion).

Um die lokalen Spam-Schutz-Filter zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Spam-Schutz**.
4. Wählen Sie im Fenster **Spam-Schutz** den Reiter **Einstellungen** aus.
5. Klicken Sie auf die Schalter, um die lokalen Spam-Filter zu aktivieren oder deaktivieren.

Wenn Sie Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird nutzen, können Sie die lokalen Spam-Filter direkt aus Ihrem Mail-Client heraus konfigurieren. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche ⚙ **Einstellungen** und wählen Sie dann den Reiter **Spam-Filter** aus.

18.7. Konfigurieren der Cloud-Einstellungen

Die Cloud-Erkennung nutzt die Bitdefender-Cloud-Dienste, um Ihnen effizienten und stets aktuellen Spam-Schutz bieten zu können.

Der Cloud-Schutz funktioniert, solange der Bitdefender-Spam-Schutz aktiviert ist.

Beispiele legitimer E-Mails und Spam-Nachrichten können an die Bitdefender-Cloud geschickt werden, wenn Sie auf Erkennungsfehler oder unerkannte Spam-Nachrichten hinweisen. Dies trägt dazu bei, die Bitdefender-Spam-Erkennung zu verbessern.

Konfigurieren Sie die Übermittlung der E-Mail-Beispiele an die Bitdefender-Cloud, indem Sie die gewünschten Optionen wie folgt auswählen:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Spam-Schutz**.
4. Wählen Sie im Fenster **Spam-Schutz** die gewünschten Optionen aus dem Reiter **Einstellungen** aus.

Wenn Sie Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird nutzen, können Sie die Cloud-Erkennung direkt aus Ihrem Mail-Client heraus konfigurieren. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Einstellungen** und wählen Sie dann den Reiter **Cloud-Einstellungen** aus.

19. INTERNET-SCHUTZ

Der Bitdefender-Internet-Schutz lässt Sie sicher im Web surfen, indem er Sie vor potenziellen Phishing-Seiten warnt.

Bitdefender bietet Echtzeit-Surf-Schutz für:

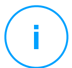
- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

So können Sie die Einstellungen für den Internet-Schutz konfigurieren:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Internet-Schutz**.

Klicken Sie auf die Schalter, um das Folgende zu aktivieren oder deaktivieren:

- Anzeige der Bitdefender-Symbolleiste im Web-Browser.



Beachten Sie

Die Bitdefender-Browser-Symbolleiste ist standardmäßig nicht aktiviert.

- Suchberater, eine Komponente, die Ihre Suchmaschinentreffer und Links auf Seiten sozialer Netzwerke analysiert und bewertet. Die Bewertung wird durch ein Symbol neben dem Link oder Treffer angezeigt:

  Sie sollten diese Webseite nicht aufrufen.

  Diese Webseite könnte gefährliche Inhalte haben. Seien Sie vorsichtig, wenn Sie sie dennoch aufrufen möchten.

  Diese Seite ist sicher.

  Der Suchberater anaylsiert die Treffer der folgenden Internet-Suchmaschinen:

  - Google
  - Yahoo!
  - Bing
  - Baidu

Der Suchberater bewertet Links, die auf den folgenden sozialen Netzwerken im Internet veröffentlicht werden:

  - Facebook
  - Twitter

- SSL-Datenverkehr-Scans.

  Gute durchdachte Angriffsversuche könnten den sicheren Datenverkehr für sich zu nutzen, um ihre Opfer zu täuschen. Darum empfiehlt es sich, den SSL-Scan zu aktivieren.

- Schutz vor Betrug.

- Schutz vor Phishing-Attacken.

Sie können eine Liste mit Websites anlegen, die nicht von den Bitdefender-Engines für den Malware-, Phishing- und Betrugsschutz gescannt werden sollen. Diese Liste sollte nur Websites enthalten, denen Sie uneingeschränkt vertrauen. Fügen Sie beispielsweise Websites hinzu, auf denen Sie häufig einkaufen.

Um Websites mithilfe des Internet-Schutzes in Bitdefender zu konfigurieren und verwalten, klicken Sie auf den Link zur **Whitelist**. Ein neues Fenster wird sich öffnen.

Um eine Website zur Whitelist hinzuzufügen, geben Sie die Adresse in das entsprechende Feld ein und klicken Sie dann auf **Hinzufügen**.

Um eine Website aus der Liste zu entfernen, wählen Sie sie aus der Liste aus und klicken Sie auf den entsprechenden **Entfernen**-Link.

Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

19.1. Bitdefender-Schutz in Ihrem Browser

Bitdefender integriert sich über eine intuitive und einfach zu bedienende Symbolleiste in die folgenden Web-Browser:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Die Bitdefender-Symbolleiste ist anders als andere Browser-Symbolleisten. Sie fügt lediglich einen kleinen Dragger zu Ihrem Browser hinzu, der am

oberen Rand jeder Webseite angezeigt wird. Klicken Sie darauf, um die Symbolleiste anzuzeigen.

Die Bitdefender-Symbolleiste enthält die folgenden Elemente:

Seitenbewertung

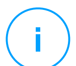
Abhängig davon, wie Bitdefender die Webseite, die sie gerade besuchen, einstuft, wird eine der folgenden Bewertungen auf der linken Seite der Symbolleiste eingeblendet:

- Die Nachricht "Seite nicht sicher" erscheint auf rotem Hintergrund - Sie sollten diese Seite umgehend verlassen. Wenn Sie mehr über diese Bedrohung erfahren möchten, klicken Sie auf das **+**-Symbol der Seitenbewertung.
- Die Nachricht "Vorsicht ist geboten" erscheint auf orangefarbenem Hintergrund erscheint - diese Webseite könnte gefährliche Inhalte enthalten. Seien Sie vorsichtig, wenn Sie sie dennoch aufrufen möchten.
- Die Nachricht "Diese Website ist sicher" erscheint auf grünem Hintergrund - Sie können diese ohne Risiko aufrufen.

Sandbox

Klicken Sie auf , um den Browser in einer von Bitdefender gestellten Umgebung zu starten und ihn so vom Betriebssystem zu isolieren. Dadurch wird verhindert, dass Browser-basierte Bedrohungen Schwachstellen in Ihrem Browser ausnutzen, um die Kontrolle über Ihr System zu erlangen. Nutzen Sie die Sandbox, wenn Sie Webseiten aufrufen, auf denen Sie Malware vermuten.

Browser-Fenster, die in der Sandbox geöffnet werden, sind leicht an der anderen Umrandung und am Sandbox-Symbol in der Mitte der Titelleiste erkennbar.



Beachten Sie

Die Sandbox ist nicht auf Computern mit Windows XP verfügbar.

Einstellungen

Klicken Sie auf , um einzelne Funktionen auszuwählen, die Sie aktivieren oder deaktivieren wollen:

- Phishing-Filter
- Malware-Web-Filter
- Suchberater

Hauptschalter

Um die Funktionen der Symbolleiste vollständig zu aktivieren oder deaktivieren, klicken Sie auf ⏻ auf der rechten Seite der Symbolleiste.

19.2. Bitdefender-Benachrichtigungen im Browser

Wenn Sie versuchen eine Website aufzurufen, die als unsicher eingestuft wurde, wird die entsprechende Website blockiert und eine Warnseite wird in Ihrem Browser angezeigt.

Die Seite enthält Informationen wie zum Beispiel die URL der Website und die erkannte Bedrohung.

Sie müssen entscheiden, wie Sie fortfahren möchten. Die folgenden Optionen sind verfügbar:

- Die Seite über einen Klick auf **Ich gehe lieber auf Nummer sicher** verlassen.
- Die Blockierung von Seiten, die Phishing-Elemente enthalten, mit einem Klick auf **Phishing-Filter deaktivieren** aufheben.
- Die Blockierung von Seiten, die Malware enthalten, mit einem Klick auf **Malware-Filter deaktivieren** aufheben.
- Fügen Sie die Seite der Phishing-Schutz-Whitelist hinzu, indem Sie auf **Zur Whitelist hinzufügen** klicken. Diese Seite wird nicht mehr von den Phishing-Schutz-Engines von Bitdefender gescannt.
- Rufen Sie die Website trotz der Warnung auf, indem Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken.

20. DATENSCHUTZ

Der Datenschutz verhindert, dass sensible Daten in fremde Hände gelangen, wenn Sie online sind.

Gehen wir von einem einfachen Beispiel aus: Sie haben eine Datenschutzregel definiert, die Ihre Kreditkartennummer schützt. Falls es eine Spyware-Software irgendwie schafft, sich auf Ihrem Computer zu installieren, kann sie Ihre Kreditkartennummer nicht per E-Mail, Sofortnachricht oder über eine Website versenden. Zudem können Ihre Kinder sie nicht benutzen, um online einzukaufen oder Sie an Personen weiterzugeben, mit denen sie im Internet Kontakt haben.

20.1. Informationen zum Datenschutz

Ob es sich um Ihre E-Mail-Adresse handelt oder um Ihre Kreditkartennummer, wenn sie in die falschen Hände geraten, können diese Informationen großen Schaden anrichten: Sie werden möglicherweise in Spam-Nachrichten ertrinken oder sich über ein geleertes Konto wundern.

Der Datenschutz durchsucht den ausgehenden Web-, E-Mail- und Sofortnachrichtenverkehr anhand der von Ihnen festgelegten Regeln nach bestimmten Zeichenfolgen (z.B. nach Ihrer Kreditkartennummer). Wenn eine Übereinstimmung mit einer Webseite, E-Mail Adresse oder IM-Nachricht gefunden wird, werden diese sofort geblockt.

Sie können Regeln erstellen, um jegliche Information zu schützen, die Sie als persönlich oder vertraulich betrachten, von Ihrer Telefonnummer oder E-Mail-Adresse bis hin zu Ihren Bankkontoangaben. Es besteht die Möglichkeit der Mehrbenutzerunterstützung, wodurch die Benutzer, die sich an den verschiedenen Windows-Benutzerkonten anmelden, Ihre eigenen Regeln konfigurieren und anwenden können. Falls Ihr Windows-Benutzerkonto ein Administratorkonto ist, können Sie festlegen, dass erstellte Regeln auch für andere Benutzer gelten, wenn diese sich unter ihrem Benutzernamen bei Windows anmelden.

20.2. Konfigurieren des Datenschutzes

Wenn Sie den Datenschutz nutzen möchten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Privatsphäre**.

3. Klicken Sie auf das Modul **Datenschutz**.
4. Stellen Sie sicher, dass der Datenschutz aktiviert ist.
5. Erstellen Sie Regeln, um wichtige Daten zu schützen. Für weitere Informationen lesen Sie bitte *„Erstellen von Datenschutzregeln“* (S. 133).

20.2.1. Erstellen von Datenschutzregeln

Um eine Regel anzulegen, klicken Sie auf **Regel hinzufügen** und folgen Sie den Anweisungen des Konfigurationsassistenten. Über die Schaltflächen **Weiter** und **Zurück** können Sie im Assistenten blättern. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Beschreibung der Regel**

   Hier können Sie die Parameter auswählen:

   - **Name der Regel** - Geben Sie einen Namen für die Regel in dieses Bearbeitungsfeld ein.
   - **Regeltyp** - Wählen Sie den Regeltyp (Adresse, Name, Kreditkarte, PIN, TAN usw.).
   - **Regeldaten** - Geben Sie hier die Daten ein, die geschützt werden sollen. Wenn Sie zum Beispiel Ihre Kreditkartennummer schützen wollen, geben Sie sie zum Teil oder ganz ein.

     Wichtig

     Wir empfehlen die Eingabe von mindestens drei Zeichen um ein versehentliches blockieren von Nachrichten oder Webseiten zu verhindern. Für mehr Sicherheit, geben Sie die Daten unvollständig ein (zum Beispiel, nur einen Teil Ihrer Kreditkartennummer).

   - **Beschreibung der Regel** - Geben Sie bitte eine kurze Beschreibung der Regel in das Editierfeld ein. Da die blockierten Daten (Zeichenfolgen) nicht als ein vollständiger Text angezeigt werden, wenn auf die Regel zugegriffen wird, sollte Ihnen die Beschreibung dabei helfen sie einfach zu identifizieren.

2. **Regel-Einstellungen konfig.**

   a. Bitte wählen Sie die Datenverkehrsart, die Bitdefender scannen soll.

      - **HTTP-Datenverkehr scannen** - Scannt den HTTP- (Web-) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.

- **E-Mails scannen (SMTP-Datenverkehr)** - Scannt den SMTP- (E-Mail-) Datenverkehr und blockiert alle ausgehenden E-Mail-Nachrichten, die den Regeln entsprechen.

Sie können wählen, ob die Regeln nur zutreffen, wenn die Daten der Regeln wörtlich übereinstimmen oder ob die komplette Zeichenfolge übereinstimmen muss.

b. Geben Sie den Benutzer an, für den die Regel angewendet werden soll.

- **Nur für mich (Aktueller Benutzer)** - Die Regel wird nur für Ihr Benutzerkonto angewandt.
- **Alle Benutzer** - Die Regel wird für alle Windows-Benutzerkonten angewandt.
- **Eingeschränkte Benutzerkonten** - Die Regel wird für Ihr Benutzerkonto und alle anderen eingeschränkten Windows-Benutzerkonten angewandt.

Klicken Sie auf **Fertigstellen.** Die Regel wird in der Tabelle erscheinen.

Ab jetzt wird jeder Versuch, die Regel über ein ausgewähltes Protokoll zu senden, fehlschlagen. Im Ereignis-Fenster wird ein Eintrag angezeigt, der darauf hinweist, dass Bitdefender das Versenden von identitätsspezifischen Inhalten blockiert hat.

20.3. Regeln bearbeiten

Verwalten Sie die Datenschutzregeln wie folgt:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Privatsphäre**.
3. Klicken Sie auf das Modul **Datenschutz**.

Sie können eine Liste der Regeln in der Aufstellung ansehen.

Um eine Regel zu löschen, markieren Sie diese und klicken dann auf die Schaltfläche **Regel löschen**.

Um eine Regel zu bearbeiten, markieren Sie diese und klicken dann auf den Button **Regel bearbeiten**. Ein neues Fenster wird sich öffnen. Hier können Sie Namen, Beschreibungen und Parameter der Regel ändern. (Typ, Daten und Datenverkehr). Klicken Sie auf **OK**, um die Änderungen zu speichern.

20.4. Endgültiges Löschen von Dateien

Wenn Sie eine Datei löschen, kann auf diese nicht mehr auf normalem Wege zugegriffen werden. Die Datei ist jedoch physisch solange weiterhin auf der Festplatte vorhanden, bis sie durch eine neue Datei überschrieben wird.

Der Bitdefender-Dateischredder hilft Ihnen, Daten endgültig zu löschen, indem er sie physisch von der Festplatte entfernt.

Wenn Sie das Windows-Kontextmenü nutzen möchten, um Dateien oder Ordner auf Ihrem Computer schnell und einfach zu schreddern, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, den Sie unwiderruflich löschen möchten.
2. Wählen Sie dann im Kontextmenü **Bitdefender** > **Dateischredder**.
3. Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **Ja**, um den Assistenten für den Dateischredder zu starten.
4. Bitte warten Sie, bis Bitdefender das Schreddern der Dateien abgeschlossen hat.
5. Die Ergebnisse werden angezeigt. Klicken Sie auf **Schließen**, um den Assistenten zu beenden.

Alternativ können Sie Dateien auch von innerhalb der Bitdefender-Benutzeroberfläche schreddern.

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Privatsphäre**.
3. Wählen Sie im Modul **Datenschutz** den Punkt **Dateischredder** aus.
4. Befolgen Sie die Anweisungen des Dateischredderassistenten:
   a. **Datei/Ordner auswählen**

      Fügen Sie die Dateien oder Verzeichnisse, die Sie endgültig entfernen möchten, hinzu.

   b. **Dateien schreddern**

      Bitte warten Sie, bis Bitdefender das Schreddern der Dateien abgeschlossen hat.

   c. **Bericht**

Die Ergebnisse werden angezeigt. Klicken Sie auf **Schließen**, um den Assistenten zu beenden.

21. SCHWACHSTELLE

Ein wichtiger Schritt für den Schutz Ihres Computers gegen Hacker und schädliche Anwendungen besteht darin, das Betriebssystem und die Programme, die Sie oft verwenden, stets auf dem neusten Stand eu halten. Sie sollten zudem in Betracht ziehen, die Windows-Einstellungen zu deaktivieren, die das System anfälliger für Malware machen. Und um einen ungewünschten Zugriff auf Ihren Computer zu vermeiden sind sichere Passwörter (Passwörter die nicht einfach umgangen werden können) für jedes Windows-Benutzerkonto notwendig.

Bitdefender überprüft Ihr System automatisch auf Schwachstellen und informiert Sie über diese. Systemschwachstellen beinhalten das Folgende:

- veraltete Anwendungen auf Ihrem Computer.
- fehlende Windows Updates.
- Schwache Windows Benutzerkonten Passwörter.

Bitdefender bietet Ihnen zwei einfache Möglichkeiten, die Schwachstellen Ihres Systems zu beheben:

- Sie können Ihr System nach Schwachstellen durchsuchen und diese Schritt für Schritt mit dem **Schwachstellen-Scan** beheben.
- Mithilfe der automatischen Schwachstellenüberwachung können Sie im Ereignis-Fenster erkannte Schwachstellen überprüfen und beheben.

Sie sollten Ihr System alle ein bis zwei Wochen nach Schwachstellen durchsuchen und diese beheben.

21.1. Scannen des Computers nach Schwachstellen

So beheben Sie Systemschwachstellen mit dem Schwachstellen-Scan:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie im Modul **Schwachstelle** auf **Schwachstellen-Scan**.
4. Bitte warten Sie, bis Bitdefender die Schwachstellenprüfung beendet hat. Klicken Sie unten im Fenster auf **Überspringen**, um den Scan-Vorgang zu beenden.

   a. **Anwendungsupdates**

Wenn eine Anwendung nicht auf dem neusten Stand ist, klicken Sie auf den zur Verfügung stehenden Link um die aktuellste Version herunterzuladen.

Klicken Sie auf **Details anzeigen**, um Informationen zu der Anwendung anzuzeigen, die aktualisiert werden muss.

b. **Windows-Updates**

Klicken Sie auf **Details anzeigen**, um die Liste aller wichtigen Windows-Updates anzuzeigen, die zur Zeit nicht auf Ihrem Computer installiert sind.

Um die Installation der gewählten Updates zu starten, klicken Sie auf **Updates installieren**. Bitte beachten Sie, dass die Installation der Updates einige Zeit in Anspruch nehmen kann und dass manche Updates einen Neustart erfordern, um die Installation abzuschließen. Falls nötig starten Sie das System sobald es Ihnen möglich ist neu.

c. **Unsichere Passwörter**

Sie können die Liste der auf Ihrem Computer konfigurierten Windows-Benutzerkonten sehen und die Sicherheit, die das jeweilige Passwort bietet.

Klicken Sie auf **Details anzeigen**, um unsichere Passwörter zu ändern. Sie können den jeweiligen Benutzer auffordern, das Passwort bei der nächsten Anmeldung zu ändern oder das Passwort an Ort und Stelle selbst ändern. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (z.B. #, $ or @).

Oben rechts im Fenster können Sie die Ergebnisse entsprechend Ihrer Anforderungen filtern.

21.2. Automatische Schwachstellenüberwachung

Bitdefender scannt Ihr System im Hintergrund regelmäßig nach Schwachstellen und erfasst alle erkannten Probleme im Ereignis-Fenster.

Um die erkannten Probleme zu untersuchen und zu beheben, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.

2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.
3. Klicken Sie im Fenster **Ereignisse** auf **Schwachstelle**.
4. Sie erhalten detaillierte Informationen zu den erkannten Systemschwachstellen. Abhängig vom Problem, um eine spezifische Schwachstelle zu beheben, gehen Sie folgendermaßen vor:
   - Falls Windows-Updates verfügbar sind, klicken Sie auf **Jetzt aktualisieren**.
   - Falls eine Anwendung nicht mehr auf dem neuesten Stand ist, klicken Sie auf **Update jetzt durchführen**, um einen Link zur Website des Anbieters zu finden, von der aus Sie die neueste Version der Anwendung installieren können.
   - Wenn ein Windows-Benutzerkonto mit einem schwachen Passwort gesichert ist, klicken Sie auf **Passwort ändern**, um den Benutzer dazu zu zwingen, das Passwort bei der nächsten Anmeldung zu ändern oder es selbst zu ändern. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (z.B. #, $ or @).
   - Sollte die Autorun-Funktion in Windows aktiviert sein, klicken Sie auf **Deaktivieren**, um es zu deaktivieren.

Um die Einstellungen für die Schwachstellenüberwachung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Schwachstelle**.
4. Klicken Sie auf den Schalter, um den Schwachstellen-Scan zu aktivieren oder deaktivieren.



Wichtig

Um automatisch über System- oder Anwendungsschwachstellen benachrichtigt zu werden, lassen Sie die Option **Schwachstellen-Scan** aktiviert.

5. Nutzen Sie die entsprechenden Schalter, um die Systemschwachstellen auszuwählen, die Sie regelmäßig überprüfen möchten.

Kritische Windows-Updates

Überprüfen Sie, ob die neuesten kritischen Microsoft-Sicherheits-Updates auf Ihrem Windows-Betriebssystem installiert sind.

Anwendungsupdates

Prüfen Sie, ob die auf Ihren System installierten Anwendungen aktuell sind. Veraltete Anwendungen können von schädlicher Software ausgenutzt werden und Ihren PC so anfällig für Angriffe von außen machen.

Unsichere Passwörter

Überprüfen Sie, ob die Passwörter der Windows-Benutzerkonten, leicht zu erraten sind oder nicht. Passwörter, die schwer zu erraten sind (starke Passwörter), mache es sehr schwierig für Hacker, in Ihr System einzudringen. Ein starkes Passwort sollte aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen (z.B. #, $ oder @) bestehen.

Medien-Autostart

Überprüfen Sie den Status der Windows-Autorun-Funktion. Mit dieser Funktion lassen sich Anwendungen automatisch direkt von CD, DVD, USB-Stick oder anderen externen Speichermedien starten.

Manche Malware-Arten verbreiten sich über den Autostart von Wechselmedien auf Ihrem PC. Aus diesem Grund sollten Sie diese Windows-Funktion deaktivieren.



Beachten Sie

Wenn Sie die Überwachung einer bestimmten Schwachstelle deaktivieren, werden damit zusammenhängende Ereignisse nicht mehr im Ereignisfenster erfasst.

22. FIREWALL

Die Firewall schützt Ihren Computer vor unerwünschten Verbindungen von innen und außen sowohl im lokalen Netzwerk als auch im Internet. Sie funktioniert im Prinzip wie ein Wächter an Ihrem Tor - sie überwacht alle Verbindungsversuche und entscheidet, welche Verbindungen zugelassen und welche blockiert werden.

Die Bitdefender-Firewall nutzt eine Regelwerk, um den eingehenden und ausgehenden Datenverkehr auf Ihrem System zu filtern. Die Regeln sind in zwei Kategorien unterteilt:

Allgemeine Regeln

Regeln, mit denen die Protokolle festgelegt werden, über die die Kommunikation stattfinden darf.

Dabei kommt ein Standardregelwerk zum Einsatz, das optimalen Schutz gewährleistet. Sie können die Regeln bearbeiten, indem Sie Verbindungen über bestimmte Protokolle zulassen oder verweigern.

Anwendungsregeln

Regeln, die festlegen, wie jede einzelne Anwendung auf Netzwerkressourcen und das Internet zugreifen kann.

Unter normalen Umständen legt Bitdefender automatisch eine Regel an, sobald eine Anwendung versucht, auf das Internet zuzugreifen. Sie können Anwendungsregeln zudem manuell hinzufügen oder bearbeiten.

Wenn auf Ihrem Computer Windows Vista, Windows 7 oder Windows 8 läuft, wird Bitdefender automatisch jeder erkannten Netzwerkverbindung den entsprechenden Netzwerktyp zuordnen. Je nach Netzwerktyp wird der Firewall-Schutz für jede Verbindung auf die angemessene Stufe eingestellt.

Um mehr über die Firewall-Einstellungen für jeden Netzwerktyp und die Bearbeitung der Netzwerkeinstellungen zu erfahren, lesen Sie bitte das Kapitel *„Verbindungseinstellungen verwalten“* (S. 146).

22.1. Aktivieren / Deaktivieren des Firewall-Schutzes

Um den Firewall-Schutz zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.

3. Klicken Sie auf das Modul **Firewall**.
4. Klicken Sie im Fenster **Firewall** auf den Firewall-Schalter.



Warnung

Die Deaktivierung der Firewall sollte immer nur von kurzer Dauer sein, da Ihr Computer so der Gefahr durch nicht autorisierte Verbindungen ausgesetzt wird. Aktivieren Sie die Firewall so schnell wie möglich wieder.

22.2. Firewall-Regeln verwalten

22.2.1. Allgemeine Regeln

Wenn Daten über das Internet übertragen werden, werden bestimmte Protokolle genutzt.

Über die allgemeinen Regeln können Sie die Protokolle konfigurieren, über die Datenverkehr stattfinden darf. Allgemeine Regeln werden beim Öffnen der Firewall standardmäßig nicht angezeigt. Um die Regeln zu bearbeiten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Firewall**.
4. Wählen Sie im Fenster **Firewall** den Reiter **Regeln** aus.
5. Aktivieren Sie das Kästchen **Allgemeine Regeln anzeigen** unten Links im Fenster.

Die Standardregeln werden angezeigt. Um die Priorität einer Regel zu bearbeiten, klicken Sie in der Spalte **Berechtigung** auf den entsprechenden Pfeil und wählen Sie **Zulassen** oder **Verweigern**.

DNS über UDP / TCP

DNS über UDP und TCP zulassen oder verweigern.

Diese Verbindungsart wird standardmäßig zugelassen.

Eingehende ICMP / ICMPv6

ICMP- / ICMPv6-Nachrichten zulassen oder verweigern.

ICMP-Nachrichten werden häufig von Hackern für Angriffe auf Computer-Netzwerke genutzt. Diese Verbindungsart wird standardmäßig verweigert.

Versenden von E-Mails
Versand von E-Mails über SMTP zulassen oder verweigern.

Diese Verbindungsart wird standardmäßig zugelassen.

Web-Browsing HTTP
HTTP-Browsing zulassen oder verweigern.

Diese Verbindungsart wird standardmäßig zugelassen.

Eingehende Remote-Desktop-Verbindungen
Den Zugriff anderer Computer über Remote-Desktop-Verbindungen zulassen oder verweigern.

Diese Verbindungsart wird standardmäßig zugelassen.

Windows-Explorer-Datenverkehr auf HTTP / FTP
HTTP- und FTP-Datenverkehr aus Windows Explorer heraus zulassen oder verweigern.

Diese Verbindungsart wird standardmäßig verweigert.

22.2.2. Anwendungsregeln

So können Sie die Firewall-Regeln anzeigen und verwalten, die den Zugang von Anwendungen zu Netzwerkressourcen und dem Internet steuern:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Firewall**.
4. Wählen Sie im Fenster **Firewall** den Reiter **Regeln** aus.

Sie können die Programme (Prozesse), für die Firewall-Regel erstellt wurde, in der Tabelle sehen. Um die erstellten Regeln für eine bestimmte Anwendung anzuzeigen, müssen Sie diese nur doppelt anklicken.

Für jede Regel werden die folgenden Informationen angezeigt:

- **Name** - Name des Prozesses, auf den die Regel angewendet werden soll.
- **Netzwerktypen** - Die Prozess- und Netzwerkadaptertypen, auf die die Regel angewendet wird. Regeln werden automatisch erstellt um den Netzwerk- oder Internetzugriff jedes Adapters zu filtern. Die Regeln werden standardmäßig auf jedes Netzwerk angewendet. Sie können manuell Regeln erstellen oder bestehende Regeln bearbeiten um den Zugriff einer

Anwendung auf das Netzwerk/Internet über einen speziellen Adapter zu filtern (zum Beispiel ein drahtloser Netzwerkadapter).

- **Protokoll** - Das IP-Protokoll, auf das die Regel angewendet wird. Die Regeln werden standardmäßig auf jedes Protokoll angewendet.
- **Berechtigung** - Gibt an, ob der Zugriff der Anwendung auf das Netzwerk oder das Internet unter den festgelegten Umständen zugelassen oder verweigert wird.

Verwalten Sie die Regeln mithilfe der Schaltflächen oberhalb der Tabelle:

- **Regel hinzufügen** - Öffnet ein Fenster, in dem eine neue Regel erstellt werden kann.
- **Regel entfernen** - Löscht die ausgewählte Regel.
- **Regeln zurücksetzen** - Öffnet ein Fenster, in dem Sie die bestehenden Regeln entfernen und die Standardregeln wiederherstellen können.

Anwendungsregeln hinzufügen / bearbeiten

Um eine Anwendungsregel hinzuzufügen oder zu bearbeiten, klicken Sie oberhalb der Tabelle auf die Schaltfläche **Regel hinzufügen** oder klicken Sie auf eine bestehende Regel. Ein neues Fenster wird sich öffnen. Gehen Sie wie folgt vor:

- **Programmpfad.** Klicken Sie auf **Durchsuchen** und wählen Sie das Programm für das die Regel angewendet wird.
- **Lokale Adresse.** Geben Sie die lokale IP-Adresse und den Port an, auf den die Regel angewendet werden soll. Wenn Sie mehr als einen Netzwerkadapter haben, können sie die Markierung im Kästchen **Alle** aufheben und eine bestimmte IP-Adresse eingeben.
- **Remote-Adresse.** Geben Sie die Remote-IP-Adresse und den Port an, auf den die Regel angewendet werden soll. Um den Datenverkehr zwischen Ihrem Computer und einem bestimmten Computer zu filtern, lassen Sie das Kontrollkästchen **Alle** frei und geben Sie dessen IP-Adresse an.
- **IP-Version.** Wählen Sie aus dem Menu die IP-Version (IPv4, IPv6 oder andere), für die die Regel angewendet werden soll.
- **Richtung.** Wählen Sie aus dem Menu die Richtung des Datenverkehrs, für den die Regel angewendet wird.

Richtung	Beschreibung
Ausgehend	Die Regel bezieht sich nur auf den ausgehenden Datenverkehr.
Eingehend	Die Regel bezieht sich nur auf den eingehenden Datenverkehr.
Beides	Die Regel findet in beiden Richtungen Anwendung.

Klicken Sie auf den Link **Weitere Optionen**, um weitere Aktionen aufzurufen:

- **Protokoll.** Wählen Sie aus dem Menu das IP-Protokoll für das die Regel angewendet wird.
  - Wenn Sie möchten, dass die Regel für alle Protokolle angewendet wird, wählen Sie **Alle**.
  - Wenn Sie möchten, dass die Regel für TCP-Protokolle angewendet wird, wählen Sie **TCP**.
  - Wenn Sie möchten, dass die Regel für UDP-Protokolle angewendet wird, wählen Sie **UDP**.
  - Wenn Sie möchten, dass die Regel auf ein bestimmtes Protokoll angewendet wird, geben Sie die Nummer des Protokolls, das Sie filtern möchten, in das leere Feld ein.



Beachten Sie

Die Nummern von IP-Protokollen werden von der Internet Assigned Numbers Authority (IANA) zugewiesen. Die komplette Liste zugewiesener Nummern von IP-Protokollen finden Sie unter http://www.iana.org/assignments/protocol-numbers.

- **Ereignisanzeige.** Wählen Sie je nach ausgewähltem Protokoll die Netzwerkereignisse, auf die die Regel angewendet werden soll. Folgende Ereignisse können auftreten:

Ereignis	Beschreibung
Verbinden	Vorausgehender Austausch von Standardnachrichten, die von Verbindungsprotokollen (wie TCP) verwendet werden, um eine Verbindung herzustellen. Mit Verbindungsprotokollen entsteht ein Datenverkehr zwischen

Ereignis	Beschreibung
	zwei Computern nur nachdem eine Verbindung hergestellt wurde.
Datenverkehr	Datenfluss zwischen zwei Computern.
Abhören	Status in dem eine Anwendung das Netzwerk überwacht, das eine Verbindung herstellen oder Informationen über eine Peer-Anwendung erhalten möchte.

- **Netzwerktyp.** Wählen Sie den Netzwerktyp aus, auf den die Regel angewendet werden soll. Sie können den Netzwerktyp ändern, indem Sie das Dropdown-Menü unter **Netzwerktyp** öffnen und einen der verfügbaren Netzwerktypen aus der Liste auswählen.

Netzwerktyp	Beschreibung
Vertrauensw.	Deaktiviert die Firewall für den entsprechenden Adapter.
Heim/Büro	Erlaubt den Datenverkehr zwischen Ihrem Computer und den Computern im lokalen Netzwerk.
Öffentlich	Sämtlicher Datenverkehr wird gefiltert.
Unsicher	Der Netzwerk- und Internet-Datenverkehr über den entsprechenden Adapter wird vollständig blockiert.

- **Berechtigung.** Wählen Sie eine der verfügbaren Erlaubnis-Optionen:

Berechtigung	Beschreibung
Zulassen	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt.
Verweigern	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen verweigert.

22.3. Verbindungseinstellungen verwalten

Für jede Netzwerkverbindung können Sie spezielle vertrauenswürdige oder nicht vertrauenswürdige Zonen konfigurieren.

Ein vertrauenswürdige Zone ist ein Gerät (zum Beispiel ein anderer Computer oder ein Drucker), dem Sie uneingeschränkt vertrauen. Jeglicher Datenverkehr zwischen Ihrem Computer und einem vertrauenswürdigen Gerät wird zugelassen. Um Ressourcen mit speziellen Computern in ungesicherten WLAN-Netzwerken zu teilen, fügen Sie sie als erlaubte Computer hinzu.

Eine nicht vertrauenswürdige Zone ist ein Gerät, das mit Ihrem Computer unter keinen Umständen kommunizieren soll.

Um die Zonen in Ihren Netzwerkadaptern anzuzeigen und zu verwalten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Firewall**.
4. Wählen Sie im Fenster **Firewall** den Reiter **Adapter** aus.

Ein neues Fenster wird angezeigt, in dem die Netzwerkadapter mit aktiven Verbindungen und aktuellen Zonen, falls vorhanden, angezeigt werden:

Für jede Zone werden die folgenden Informationen angezeigt:

- **Netzwerktyp** - Der Netzwerktyp, mit dem Ihr Computer verbunden ist.
- **Stealth Modus** - Ob Sie von anderen Computern entdeckt werden können.

  Die Tarnkappe können Sie über die gewünschte Option aus dem entsprechenden Klappmenü konfigurieren.

Stealth-Option	Beschreibung
An	Stealth-Modus ist aktiviert. Ihr Computer ist sowohl im lokalen Netzwerk als auch im Internet unsichtbar.
Aus	Stealth-Modus ist deaktiviert. Jeder Benutzer im lokalen Netzwerk oder im Internet kann Ihren Computer entdecken.
Remote	Ihr Computer kann nicht im Internet entdeckt werden. Benutzer im lokalen Netzwerk können Ihren Computer entdecken

- **Allgemein** - ob die allgemeinen Regeln für diese Verbindung angewendet werden sollen.

  Wenn sich die IP-Adresse eines Netzwerkadapters geändert hat, verändert Bitdefender die Vertrauensstufe entsprechend. Wenn Sie den Netzwerktyp beibehalten möchten, wählen Sie im entsprechenden Klappmenü **Ja**.

Hinzufügen / Bearbeiten von Ausnahmen

Um eine Ausnahme hinzuzufügen oder zu bearbeiten, klicken Sie oberhalb der Tabelle auf **Netzwerkausnahmen**. Ein neues Fenster mit den IP-Adressen der mit dem Netzwerk verbundenen Geräte wird angezeigt. Gehen Sie wie folgt vor:

1. Wählen Sie die IP-Adresse des Computers, den Sie hinzufügen wollen, aus oder geben Sie eine Adresse oder einen Adressbereich in das entsprechende Textfeld ein.
2. Wählen Sie die Berechtigung aus:
   - **Erlauben** - jeglicher Datenverkehr zwischen Ihrem Computer und dem ausgewählten Computer wird erlaubt.
   - **Verweigern** - jeglicher Datenverkehr zwischen Ihrem Computer und dem ausgewählten Computer wird blockiert.
3. Klicken Sie auf die Schaltfläche **+**, um die Ausnahme hinzuzufügen und das Fenster zu schließen.

   Klicken Sie zur Entfernung einer IP auf die entsprechende Schaltfläche und schließen Sie das Fenster.

22.4. Konfigurieren der erweiterten Einstellungen

So können Sie erweiterte Firewall-Einstellungen vornehmen:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Firewall**.
4. Wählen Sie im Fenster **Firewall** den Reiter **Einstellungen** aus.

Die folgenden Funktionen können aktiviert oder deaktiviert werden.

- **Gemeinsame Nutzung der Internetverbindung** - Aktiviert die Unterstützung für die gemeinsame Nutzung der Internetverbindung.



Beachten Sie
Diese Option aktiviert die **gemeinsame Nutzung derInternetverbindung (ICS)** nicht automatisch auf Ihrem System, sondern macht diese Art der Verbindung nur möglich, wenn Sie es von Ihrem Betriebssystem aus aktivieren.

- **Port-Scans im Netzwerk blockieren** - Erkennt und blockiert Versuche offene Ports zu finden.

  Portscans werden von Hackern verwendet, um herauszufinden, welche Ports auf Ihrem Computer geöffnet sind. Wenn Sie dann einen unsicheren Port finden, können Sie in Ihren Computer eindringen.

- **WLAN-Verbindungen überwachen** - Wenn Sie mit einem Drahtlosnetzwerk verbunden sind, werden Benachrichtigungen über bestimmte Netzwerkereignisse angezeigt (z.B. wenn ein neuer Computer mit dem Netzwerk verbunden wurde).

22.5. Benachrichtigungsintensität einstellen

Bitdefender Internet Security 2015 ist darauf ausgelegt, so unauffällig wie möglich zu arbeiten. Unter normalen Umständen müssen Sie nicht entscheiden, ob Verbindungen oder Aktionen, die von den Anwendungen auf Ihrem System ausgeführt werden, zugelassen oder verweigert werden.

Wenn Sie alle Entscheidungen selbst treffen wollen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Allgemeine Einstellungen** aus.
4. Aktivieren Sie den **Paranoidmodus**, indem Sie auf den entsprechenden Schalter klicken.



Beachten Sie
Bei Aktivierung des Paranoiamodus werden der Autopilot und die Profile-Funktionen automatisch deaktiviert.
Der **Paranoiamodus** kann während des **Akkubetriebs** verwendet werden.

Während der Paranoiamodus aktiviert ist, werden Sie grundsätzlich zur Auswahl einer Aktion aufgefordert, wenn eine der folgenden Situationen eintritt:

- Eine Anwendung versucht, eine Verbindung mit dem Internet herzustellen.
- Eine Anwendung versucht eine Aktion auszuführen, die vom Angriffserkennung oder von Active Virus Control als verdächtig eingestuft wurde.

In der Benachrichtigung finden Sie detaillierte Informationen über die Anwendung und das erkannte Verhalten. Klicken Sie auf die entsprechende Schaltfläche, um **Zulassen** oder **Verweigern** für die Aktion auszuwählen.

23. ANGRIFFSERKENNUNG

Die Bitdefender-Angriffserkennung überwacht das Netzwerk und die Systemaktivitäten auf Malware-Aktivitäten oder Richtlinienverletzungen. Es erkennt und blockiert Versuche, kritische Systemdateien, Bitdefender-Dateien und Registry-Einträge zu verändern. Darüber hinaus erkennt es die Installation von Malware-Treibern und Angriffe durch Code-Injektionen (DLL-Injektionen).

So konfigurieren Sie die Angriffserkennung:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Angriffserkennung**.
4. Klicken Sie auf den entsprechenden Schalter, um die Angriffserkennung zu aktivieren.
5. Schieben Sie den Regler in die gewünschte Schutzstufenposition. Nutzen Sie die Beschreibung auf der rechten Seite der Skala, um die Stufe zu wählen, die für Ihre Sicherheitsbedürfnisse am besten geeignet ist.

Im Ereignis-Fenster können Sie überprüfen, welche Anwendungen von der Angriffserkennung erkannt wurden.

Sie können für Anwendungen, denen Sie vertrauen und die daher nicht von der Angriffserkennung gescannt werden sollen, Ausschlussregeln festlegen. Um eine Anwendung vom Scan auszuschließen, befolgen Sie die Anweisungen im Kapitel *„Verwalten von ausgeschlossenen Prozessen“* (S. 116).



Beachten Sie

Die Ausführung der Angriffserkennung steht im Zusammenhang mit der Ausführung von Active Virus Control. Ausschlussregeln für Prozesse gelten für beide Systeme.

24. SICHERE ONLINE-TRANSAKTIONEN MIT SAFEPAY

Immer mehr Menschen nutzen ihren Computer regelmäßig für ihre Einkäufe und Bankgeschäfte. Rechnungen bezahlen, Überweisungen tätigen und einkaufen war noch nie schneller und einfacher.

Bei diesen Transaktionen werden personenbezogene Daten, Konto- und Kreditkartennummern, Passwörter und andere vertrauliche Informationen über das Internet übermittelt. Und das sind genau die Daten, die Online-Kriminelle so gerne in die Finger kriegen würden. Hacker lassen nichts unversucht, an diese Daten zu gelangen. Sie können also bei der Absicherung Ihrer Online-Transaktionen gar nicht vorsichtig genug sein.

Bitdefender Safepay™ ist zuallererst ein gesicherter Browser, ein abgeschottetes System, das speziell entwickelt wurde, damit Online-Transaktionen wie Einkäufe und Bankgeschäfte sicher und privat bleiben.

Um optimalen Privatsphärenschutz zu gewährleisten, wurde die Bitdefender-Geldbörse in Bitdefender Safepay™ integriert, um Ihre Anmeldedaten jederzeit beim Aufrufen von privaten Seiten zu schützen. Für weitere Informationen lesen Sie bitte *„Die Geldbörse schützt Ihre Anmeldedaten“* (S. 157).

Bitdefender Safepay™ hat die folgenden Vorteile:

- Es blockiert den Zugriff auf Ihren Desktop sowie sämtliche Versuche, Bildschirmfotos zu machen.
- Es schützt Ihre Passwörter wenn Sie mit der Geldbörse im Internet surfen.
- Es hat eine eingebaute virtuelle Tastatur, die es Hackern unmöglich macht, Ihre Tastenanschläge aufzuzeichnen.
- Es ist völlig unabhängig von Ihren anderen Browsern.
- Es enthält den Hotspot-Schutz für Situationen, in denen Ihr Computer mit einem ungesicherten Funknetzwerk verbunden ist.
- Es hat eine Lesezeichenfunktion, mit der Sie mühelos auf Ihre Lieblings-Banking/Shopping-Seiten zugreifen können.
- Es ist nicht nur auf Online-Banking und -Shopping beschränkt. Jede Webseite kann in Bitdefender Safepay™ geöffnet werden.

24.1. Bitdefender Safepay™ verwenden

Standardmäßig erkennt Bitdefender, wenn Sie auf Ihrem Computer über einen Browser eine Online-Banking-Seite oder einen Online-Shop aufrufen und fordert Sie auf, diese Seite in Bitdefender Safepay™ zu öffnen.

Es gibt verschiedene Möglichkeiten, das Bitdefender Safepay™-Hauptfenster zu öffnen:

- Über die Bitdefender-Benutzeroberfläche:
  1. Öffnen Sie das Bitdefender-Fenster.
  2. Klicken Sie auf die **Safepay**-Schaltfläche auf der rechten Seite des Fensters.
- In Windows:
  - Für **Windows XP**, **Windows Vista** und **Windows 7**:
    1. Klicken Sie auf **Start** und **Alle Programme**.
    2. Klicken Sie auf **Bitdefender**.
    3. Klicken Sie auf **Bitdefender Safepay™**. Noch schneller geht es, wenn Sie in der Bitdefender-Benutzeroberfläche rechts auf die **Safepay**-Schaltfläche klicken.
  - In **Windows 8**:

    Finden Sie Bitdefender Safepay™ auf der Windows-Startseite (z.B. durch die Eingabe von "Bitdefender Safepay™" auf der Startseite) und rechtsklicken Sie auf das Symbol. Alternativ können Sie in der Bitdefender-Benutzeroberfläche auch rechts auf die **Safepay**-Schaltfläche klicken.



Beachten Sie

Falls das Adobe Flash Player Plugin nicht installiert oder nicht mehr aktuell ist, wird eine Bitdefender-Meldung angezeigt. Klicken Sie auf die entsprechende Schaltfläche, um fortzufahren.
Nach Abschluss des Installationsvorgangs müssen Sie den Bitdefender Safepay™-Browser erneut öffnen, um mit Ihrer Arbeit fortzufahren.

Wer schon einmal einen Internet-Browser benutzt hat, wird mit Bitdefender Safepay™ keinerlei Probleme haben - es sieht aus wie ein Browser und verhält sich auch so:

- Sie können URLs in die Adressleiste eingeben, um auf die entsprechende Seite zu gelangen.
- Sie können im Fenster von Bitdefender Safepay™ mehrere Reiter öffnen, indem Sie auf klicken.
- Sie können über die Schaltflächen rückwärts und vorwärts durch bereits besuchte Seiten blättern und Seiten neu laden.
- Sie können die Einstellungen für Bitdefender Safepay™ mit einem Klick auf aufrufen.
- schützen Sie Ihre Passwörter mit der Geldbörse durch einen Klick auf .
- Sie können Ihre Lesezeichen mit einem Klick auf neben der Adressleiste verwalten.
- Sie können eine virtuelle Tastatur über die Schaltfläche öffnen.
- die Größe des Browser-Fensters durch gleichzeitiges Drücken von **Strg** und den **+/-**-Tasten im numerischen Tastenblock anpassen.

24.2. Einstellungen verändern

Über die Schaltfläche können Sie die folgenden Einstellungen verändern:

Allgemeines Verhalten von Bitdefender Safepay™

Hier können Sie einstellen, was passiert, wenn Sie die Seite eines Online-Shops oder eine Internet-Banking-Seite in einem normalen Browser aufrufen:

- Automatisch in Bitdefender Safepay™ öffnen.
- Bitdefender soll Sie jedes Mal fragen, wie Sie vorgehen möchten.
- Bitdefender Safepay™ nie für Seiten verwenden, die in einem normalen Browser geöffnet werden.

Domain-Liste

Hier können Sie einstellen, wie Bitdefender Safepay™ sich verhalten soll, wenn Sie Webseiten bestimmter Domains in Ihrem Standardbrowser aufrufen. Fügen Sie dazu einzelne Domains der Liste hinzu, und wählen Sie für jede eines der folgenden Verhalten:

- Automatisch in Bitdefender Safepay™ öffnen.
- Bitdefender soll Sie jedes Mal fragen, wie Sie vorgehen möchten.
- Bitdefender Safepay™ beim Aufruf von Seiten dieser Domain in einem Standardbrowser nie benutzen.

Blockieren von Pop-ups

Pop-ups können Sie mit einem Klick auf den entsprechenden Schalter blockieren.

Sie können auch eine Liste mit Websites anlegen, die Pop-ups anzeigen dürfen. Diese Liste sollte nur Websites enthalten, denen Sie uneingeschränkt vertrauen.

Um eine Website zu der Liste hinzuzufügen, geben Sie die Adresse in das entsprechende Feld ein und klicken Sie dann auf **Domain hinzufügen**.

Um eine Website aus der Liste zu entfernen, wählen Sie sie aus der Liste aus und klicken Sie auf den entsprechenden **Entfernen**-Link.

24.3. Lesezeichen verwalten

Wenn Sie die automatische Erkennung einiger oder aller Websites deaktiviert haben oder Bitdefender einfach bestimmte Websites nicht korrekt erkennt, können Sie in Bitdefender Safepay™ Lesezeichen anlegen und so in Zukunft häufig besuchte Seiten schneller aufrufen.

So fügen Sie eine URL zu den Lesezeichen von Bitdefender Safepay™ hinzu:

1. Klicken Sie auf  neben der Adressleiste, um die Lesezeichenliste zu öffnen.

   Beachten Sie
   Die Lesezeichenliste wird standardmäßig geöffnet, wenn Sie Bitdefender Safepay™ starten.

2. Klicken Sie auf das **+** um ein neues Lesezeichen hinzuzufügen.
3. Geben Sie die URL und den Titel für das Lesezeichen ein, und klicken Sie anschließend auf **Erstellen**. Die URL wird auch in der Domain-Liste auf der Seite Einstellungen hinzugefügt.

24.4. Hotspot-Sicherheit in ungesicherten Netzwerken

Wenn Sie Bitdefender Safepay™ in einem ungesicherten Funknetzwerk nutzen (z. B. an einem öffentlichen Hotspot) kann die Funktion Hotspot-Schutz zusätzliche Sicherheit bieten. Dieser Dienst verschlüsselt die Internetkommunikation über ungesicherte Verbindungen, sodass Ihre Privatsphäre geschützt bleibt, ganz gleich, in welchem Netzwerk Sie sich befinden.

Der Hotspot-Schutz funktioniert nur unter den folgenden Bedingungen:

- Sie sind über Bitdefender Internet Security 2015 bei einem MyBitdefender-Konto angemeldet.
- Ihr Computer ist mit einem ungesicherten Netzwerk verbunden.

Wenn diese Dinge gegeben sind, wird Bitdefender Sie automatisch auffordern, die gesicherte Verbindung zu nutzen, sobald Sie Bitdefender Safepay™ öffnen. Sie müssen dann lediglich Ihre MyBitdefender-Zugangsdaten eingeben, wenn Sie dazu aufgefordert werden.

Die sichere Verbindung wird aufgebaut; im Bitdefender Safepay™-Fenster wird dann eine Nachricht angezeigt, sobald die Verbindung steht. Das Symbol wird in der Adressleiste vor der URL angezeigt, wenn es sich um eine sichere Verbindung handelt.

Um das Surfen im Internet visuell ansprechender zu gestalten, können Sie **Adobe Flash**- und **Java**-Plug-ins aktivieren, indem Sie auf **Erweiterte Einstellungen anzeigen** klicken.

Sie müssen die Aktion vielleicht bestätigen.

25. DIE GELDBÖRSE SCHÜTZT IHRE ANMELDEDATEN

Wir nutzen unsere Computer, um im Internet einzukaufen, unsere Rechnungen zu bezahlen, soziale Netzwerke zu besuchen oder Sofortnachrichten zu verschicken.

Aber wie jeder weiß, kann es manchmal schwer sein, sich alle Passwörter zu merken!

Und wenn wir bei Surfen im Internet nicht vorsichtig sind, können wir unsere privaten Daten wie E-Mail-Adresse, Chat-Name oder Kreditkarteninformationen ungewollt preisgeben.

Passwörter und persönliche Daten aufzuschreiben oder auf dem Computer zu speichern, kann gefährlich sein, weil sie dort nicht vor Unbefugten sicher sind, die es auf diese Informationen abgesehen haben. Und es ist eine echte Herausforderung, sich jedes einzelne Passwort zu merken, das Sie für Ihre Online-Konten und Lieblingsseiten festgelegt haben.

Gibt es also eine Möglichkeit, unsere Passwörter zu aufzubewahren, dass wir jederzeit darauf zugreifen können? Und können wir sicher sein, dass unsere Passwörter auch geheim bleiben?

Die Geldbörse verwaltet Ihre Passwörter und hilft Ihnen, nie wieder ein Passwort zu vergessen. Zudem schützt es Ihre Privatsphäre und garantiert ein sicheres Internet-Vergnügen.

Durch die Verwendung eines Master-Passworts für den Zugriff auf Ihre Anmeldedaten schützt die Geldbörse Ihre Passwörter zuverlässig.

Um Ihre Online-Aktivitäten optimal abzusichern, ist die Geldbörse mit Bitdefender Safepay™ integriert und bietet eine einheitliche Lösung für den Schutz vor den vielen Bedrohungen, denen Ihre Daten ausgesetzt sind.

Die Geldbörse schützt die folgenden privaten Daten:

- Persönliche Daten wie zum Beispiel E-Mail-Adressen oder Telefonnummern
- Anmeldeinformationen für verschiedene Websites
- Kontonummern oder Kreditkarteninformationen
- Informationen zu E-Mail-Konten
- Anwendungspasswörter
- WLAN-Passwörter

25.1. Konfigurieren der Geldbörse

Nach Abschluss der Installation werden Sie beim Öffnen des Browsers informiert, dass die Geldbörse jetzt einsatzbereit ist.

Klicken Sie auf **Durchsuchen**, um den Installationsassistenten für die Geldbörse zu starten. Folgen Sie den Anweisungen des Assistenten, um den Installationsvorgang abzuschließen.

In diesem Schritt haben Sie zwei Optionen:

- Eine neue Geldbörsen-Datenbank erstellen, um Ihre Passwörter zu schützen.

  Während des Installationsvorgangs werden Sie aufgefordert, Ihre Geldbörse mit einem Master-Passwort zu schützen. Wählen Sie ein sicheres Passwort mit mindestens 7 Zeichen.

  Ein sicheres Passwort beinhaltet mindestens eine Zahl oder ein Sonderzeichen sowie einen Großbuchstaben. Sobald Sie ein Passwort festgelegt haben, muss jeder, der die auf die Geldbörse zugreifen will, zunächst das Passwort eingeben.

  Nach Abschluss des Installationsvorgangs sind die folgenden Einstellungen für die Geldbörse standardmäßig aktiviert:

  - **Anmeldedaten automatisch in der digitalen Geldbörse speichern**.
  - **Nach meinem Master-Passwort fragen, wenn ich mich an meinem Computer anmelde**.
  - **Die Geldbörse automatisch sperren, wenn ich meinen PC verlasse**.
- Eine bestehende Datenbank importieren, wenn Sie die Geldbörse bereits zuvor verwendet haben.

Die Geldbörse-Datenbank exportieren

Um Ihre Geldbörse-Datenbank zu exportieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Privatsphäre**.
3. Klicken Sie im Modul **Geldbörse** auf **Geldbörse exportieren**.

4. Folgen Sie den Anweisungen, um die Geldbörse-Datenbank an einen lokalen Speicherort zu exportieren.

Neue Geldbörsen-Datenbank erstellen

Um eine neue Geldbörsen-Datenbank zu erstellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Privatsphäre**.
3. Klicken Sie im Modul **Geldbörse** auf **Neue Geldbörse anlegen**.
4. Es erscheint ein Warnfenster, um Sie zu informieren, dass alle derzeit in der Geldbörse gespeicherten Daten gelöscht werden. Klicken Sie auf **Ja**, um die bestehende Datenbank endgültig zu löschen und mit den Assistenten fortzufahren. Um den Assistenten zu verlassen, klicken Sie auf **Nein**.

Geldbörse-Anmeldedaten verwalten

Um Ihre Passwörter zu verwalten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Privatsphäre**.
3. Klicken Sie im Modul **Geldbörse** auf **Geldbörse öffnen**.

Ein neues Fenster wird sich öffnen. Wählen Sie im Fenster oben die gewünschte Kategorie aus:

- Identität
- Webseiten
- Online-Banking
- E-Mail-Client
- Anwendungen
- WLAN

Hinzufügen/Bearbeiten von Anmeldedaten

- Um ein neues Passwort hinzuzufügen, wählen Sie oben die entsprechende Kategorie aus, klicken Sie auf **+ Objekt hinzufügen**, geben Sie die

Informationen in den entsprechenden Feldern ein und klicken Sie auf Speichern.

- Um ein Objekt aus der Liste zu bearbeiten, klicken Sie auf die **Bearbeiten**-Schaltfläche.
- Klicken Sie zum Verlassen auf **Abbrechen**.
- Um einen Eintrag zu entfernen, wählen Sie ihn aus, klicken Sie auf **Bearbeiten** und wählen Sie **Löschen**.

25.2. Aktivieren oder Deaktivieren des Geldbörse-Schutzes

Um den Geldbörse-Schutz zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Privatsphäre**.
3. Klicken Sie auf das Modul **Geldbörse**.
4. Klicken Sie im Fenster **Geldbörse** auf den Schalter, um die **Geldbörse** zu aktivieren oder deaktivieren.

25.3. Verwalten der Einstellungen für die Geldbörse

Um das Master-Passwort im Detail zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Privatsphäre**.
3. Klicken Sie auf das Modul **Geldbörse**.
4. Wählen Sie im Fenster **Geldbörse** den Reiter **Master-Passwort** aus.

Die folgenden Optionen sind verfügbar:

- **Nach meinem Master-Passwort fragen, wenn ich mich an meinem PC anmelde** - Sie werden aufgefordert, Ihr Master-Passwort beim Zugriff auf den Computer anzugeben.
- **Nach meinem Master-Passwort fragen, wenn ich meine Browser und Anwendungen öffne** - Sie werden aufgefordert, Ihr Master-Passwort beim Zugriff auf den Browser oder eine Anwendung anzugeben.

- **Die Geldbörse automatisch sperren, wenn ich meinen PC verlasse** - Sie werden aufgefordert, Ihr Master-Passwort anzugeben, wenn Sie nach 15 Minuten an Ihren Computer zurückkehren.



Wichtig

Merken Sie sich Ihr Master-Passwort gut oder schreiben Sie es auf und verwahren es an einem sicheren Ort. Wenn Sie Ihr Passwort vergessen haben, müssen Sie das Programm neu installieren oder den Kundendienst von Bitdefender kontaktieren.

Machen Sie es sich noch einfacher

Zur Auswahl der Browser oder Anwendungen, die mit der Geldbörse integriert werden sollen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Privatsphäre**.
3. Klicken Sie auf das Modul **Geldbörse**.
4. Wählen Sie im Fenster **Geldbörse** den Reiter **Erweiterte Apps** aus.

   Wählen Sie eine Anwendung für die Nutzung der Geldbörse aus und machen Sie es sich noch einfacher:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay
   - Yahoo! Messenger
   - Skype

Konfigurieren des automatischen Einfügens

Die Funktion für das automatische Einfügen erleichtert Ihnen den Zugriff auf Ihre Lieblingsseiten und das Anmelden bei Ihren Online-Konten. Ihre Anmeldedaten und persönlichen Daten werden bei der ersten Eingabe in Ihrem Web-Browser automatisch in der Geldbörse sicher gespeichert.

Um die Einstellungen für das **automatische Einfügen** zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Privatsphäre**.
3. Klicken Sie auf das Modul **Geldbörse**.
4. Wählen Sie im Fenster **Geldbörse** den Reiter **Einstellungen für das automatische Einfügen** aus.
5. Entscheiden Sie sich für eine der folgenden Optionen:
   - **Anmeldedaten automatisch einfügen**:
     - **Anmeldedaten immer automatisch einfügen** - Die Anmeldedaten werden automatisch im Browser eingefügt.
     - **Jedes Mal nachfragen, ob meine Anmeldedaten automatisch eingefügt werden sollen** - Sie entscheiden, ob Ihre Anmeldedaten automatisch im Browser eingefügt werden.
   - **Legen Sie fest, wie die digitale Geldbörse Ihre Anmeldedaten absichern soll**:
     - **Anmeldedaten automatisch in der digitalen Geldbörse speichern** - Anmeldedaten und andere persönlich identifizierbare Daten wie Personendaten oder Kreditkarteninformationen werden in der Geldbörse automatisch gespeichert und aktualisiert.
     - **Immer fragen** - Sie werden jedes Mal gefragt, ob Ihre Anmeldedaten zur Geldbörse hinzugefügt werden sollen.
     - **Nicht speichern, ich möchte die Informationen manuell aktualisieren** - Die Anmeldedaten können nur von Hand zur Geldbörse hinzugefügt werden.
   - **Formulare automatisch ausfüllen**:
     - **Auf Formularseiten meine Ausfülloptionen anzeigen** - Ein Pop-up-Fenster mit Ihren Ausfülloptionen wird angezeigt, sobald Bitdefender erkennt, dass Sie eine Online-Zahlung vornehmen oder sich anmelden wollen.

Geldbörse-Informationen über Ihren Browser verwalten

Sie können die Geldbörse direkt über Ihren Browser verwalten, um jederzeit auf alle wichtigen Daten zugreifen zu können. Das Geldbörse-Add-on wird von den folgenden Browsern unterstützt: Google Chrome, Internet Explorer und Mozilla Firefox. Darüber hinaus ist es auch in Safepay integriert.

Um auf die Geldbörse-Erweiterung zugreifen zu können, öffnen Sie Ihren Web-Browser, stimmen Sie der Installation des Add-ons zu und klicken Sie in der Symbolleiste auf das -Symbol.

Die Geldbörse-Erweiterung bietet die folgenden Optionen:

- Geldbörse öffnen - Öffnet die Geldbörse.
- Geldbörse sperren - Sperrt die Geldbörse.
- Webseiten - Öffnet ein Untermenü mit allen in der Geldbörse gespeicherten Website-Anmeldedaten. Klicken Sie auf **Webseite hinzufügen**, um neue Websites zu der Liste hinzuzufügen.
- Formulare ausfüllen - Öffnet ein Untermenü mit den Informationen, die Sie für eine bestimmte Kategorie hinzugefügt haben. Hier können Sie neue Daten zu Ihrer Geldbörse hinzufügen.
- Einstellungen - Öffnet das Fenster für die Geldbörse-Einstellungen.
- Problem melden - Hier können Sie alle Probleme melden, die im Zusammenhang mit der Bitdefender-Geldbörse auftreten.

26. JUGENDSCHUTZ

Die Kindersicherung gibt Ihnen die Möglichkeit den Zugriff auf das Internet und auf bestimmte Programme für jeden Benutzer mit einem Benutzerkonto auf dem System zu kontrollieren.

Wenn Sie die Kindersicherung konfiguriert haben, können Sie ganz einfach herausfinden, was Ihre Kinder mit dem Computer machen.

Sie benötigen nur einen Computer mit Internetzugang und einen Webbrowser.

Sie können die Kindersicherung so konfigurieren, dass Folgendes blockiert wird:

- Unangemessene Webseiten.
- Den Internet-Zugang zu bestimmten Zeiten (beispielsweise während Unterrichtszeiten).
- Anwendungen wie Spiele, Chat, Filesharing-Programme oder Andere.
- Sofortnachrichten, die von nicht erlaubten IM-Kontakten gesendet werden.

Über MyBitdefender können Sie von jedem beliebigen Computer oder Mobilgerät mit Internetzugang die Online-Aktivitäten Ihrer Kinder überwachen und die Einstellungen der Kindersicherung verändern.

26.1. Das Kindersicherungs-Dashboard

Das Dashboard der Kindersicherung ist in Module unterteilt, über die Sie die Aktivitäten Ihrer Kinder auf dem Computer überwachen können.

Mit Bitdefender können Sie den Zugriff Ihrer Kinder auf das Internet sowie auf bestimmte Anwendungen steuern. Außerdem können Sie ihre Facbook-Aktivitäten überwachen.

Mit Bitdefender können Sie über Ihr MyBitdefender-Konto von jedem Computer oder Mobilgerät mit Internetzugang aus die Einstellungen der Kindersicherung verändern.

Sie haben zwei Möglichkeiten, Ihr Online-Konto aufzurufen:

- Von einem beliebigen Gerät mit Internetzugang aus:
  1. Öffnen Sie einen Web-Browser.
  2. Gehen Sie zu:https://my.bitdefender.com

3. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Ihrem Konto an.
4. Klicken Sie auf **Kindersicherung**, um das Dashboard zu öffnen.

- Über Ihre Bitdefender-Benutzeroberfläche:
  1. Stellen Sie sicher, dass Sie auf dem Computer eingeloggt sind, auf dem sich das Administrator-Benutzerkonto befindet. Nur Benutzer mit administrativen Rechten (Systemadministratoren) können auf die Kindersicherung zugreifen und sie konfigurieren.
  2. Öffnen Sie das Bitdefender-Fenster.
  3. Öffnen Sie den Bereich **Privatsphäre**.
  4. Wählen Sie im Modul **Kindersicherung Konfigurieren** aus.

     Stellen Sie sicher, dass Sie bei Ihrem MyBitdefender-Konto angemeldet sind.
  5. Das Kindersicherungs-Dashboard wird in einem neuen Fenster geöffnet. Hier können Sie die Einstellungen der Kindersicherung für jedes Windows-Benutzerkonto überprüfen und konfigurieren.

26.2. Profile Ihrer Kinder anlegen

Bevor Sie mit der Konfiguration der Kindersicherung fortfahren, erstellen Sie bitte für jedes Kind ein separates Benutzerkonto. Dadurch wissen Sie genau, was jedes Ihrer Kinder auf dem Computer macht. Sie sollten eingeschränkte Benutzerkonten (Standardkonten) erstellen, sodass Ihre Kinder die Einstellungen der Kindersicherung nicht ändern können. Für weitere Informationen lesen Sie bitte *„Wie lege ich Windows-Benutzerkonten an?“* (S. 71).

So können Sie das Profil Ihres Kindes in der Kindersicherung anlegen:

1. Öffnen Sie das Dashboard der Kindersicherung über Ihr MyBitdefender-Konto.
2. Klicken Sie im Menü links auf **Kind hinzufügen**.
3. Geben Sie den Namen und das Alter des Kindes in den entsprechenden Feldern ein. Durch die Angabe des Kindesalters werden automatisch für diese Altersstufe als geeignet eingeschätzte Einstellungen geladen. Diese Einstellungen basieren auf der Standard-Entwicklung von Kindern.

4. Unten werden die Geräte angezeigt, die mit Ihrem MyBitdefender-Konto verknüpft sind.
5. Wählen Sie den Computer und das Windows-Konto Ihres Kindes.
6. Klicken Sie auf **Profil anlegen**.

   Der Computer und das Windows-Konto Ihres Kindes ist jetzt mit Ihrem MyBitdefender-Konto verknüpft.

26.2.1. Installation der Kindersicherung auf Android-Geräten

Um die Kindersicherung auf dem Mobilgerät Ihres Kindes zu installieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Dashboard der Kindersicherung über Ihr MyBitdefender-Konto.
2. Klicken Sie im Menü links auf **Kind hinzufügen**.
3. Geben Sie den Namen und das Alter des Kindes in den entsprechenden Feldern ein. Durch die Angabe des Kindesalters werden automatisch für diese Altersstufe als geeignet eingeschätzte Einstellungen geladen. Diese Einstellungen basieren auf der Standard-Entwicklung von Kindern.
4. Klicken Sie zum Fortfahren auf **Auf einem neuen Gerät installieren**.
5. Ein neues Fenster wird sich öffnen. Wählen Sie **Google Play** aus der Liste.
6. Um die Kindersicherung herunterzuladen und auf dem Gerät zu installieren, klicken Sie auf **Installieren**.
7. Wählen Sie das Gerät aus, auf dem Sie die App installieren möchten.
8. Klicken Sie zum Fortfahren auf **Installieren.**

   Warten Sie, bis die App auf dem Gerät installiert wurde. Stellen Sie sicher, dass das Gerät Ihres Kindes mit dem Internet verbunden ist.
9. Nach Abschluss der Installation werde Sie aufgefordert, der Anwendung auf dem Gerät Administratorrechte einzuräumen.
10. Tippen Sie auf **Akzeptieren**, um die Installation abzuschließen.

Verknüpfen der Kindersicherung mit MyBitdefender

Um die Online-Aktivitäten Ihres Kindes zu überwachen, müssen Sie das Gerät Ihres Kindes mit Ihrem MyBitdefender-Konto verknüpfen, indem Sie sich über die App bei Ihrem Konto anmelden.

Um das Gerät mit Ihrem MyBitdefender-Konto zu verknüpfen, gehen Sie folgendermaßen vor:

1. Geben Sie Ihren MyBitdefender-Benutzernamen und Ihr Passwort ein.

   Wenn Sie noch Benutzerkonto haben, können Sie über die entsprechende Schaltfläche ein neues Konto anlegen.



Beachten Sie
Sie können auch Namen für die Geräte vergeben. Das kann sinnvoll sein, wenn Sie mehrere Geräte mit Ihrem Konto verknüpfen.

2. Tippen Sie auf **Anmelden**.

   Das Gerät Ihres Kindes ist jetzt mit Ihrem MyBitdefender-Konto verknüpft und Sie können mit der Überwachung der Online-Aktivitäten beginnen.

26.2.2. Überwachen der Aktivitäten Ihrer Kinder

Mit Bitdefender können Sie jederzeit nachvollziehen, was Ihre Kinder im Internet machen.

Sie können aufzeichnen, welche Websites sie besuchen, welche Anwendungen sie gestartet haben und welche Aktivitäten von der Kindersicherung blockiert wurden.

Die erstellten Berichte enthalten detaillierte Informationen zu jedem Vorgang:

- Der Status des Vorgangs.
- Der Name der blockierten Website.
- Der Name der blockierten Anwendung.
- Der Name des Geräts.
- Zeitpunkt, zu dem der Vorgang passiert ist.
- Die Aktionen, die Bitdefender ausgeführt hat.

So können Sie den Internet-Datenverkehr, die gestarteten Anwendungen und die Facebook-Aktivität Ihrer Kinder überwachen:

1. Öffnen Sie das Dashboard der Kindersicherung über Ihr MyBitdefender-Konto.
2. Klicken Sie auf , um das Aktivitätsfenster des entsprechenden Moduls zu öffnen.

26.2.3. Konfigurieren der allgemeinen Einstellungen

- Aktivitätsberichte

  Standardmäßig werden bei aktivierter Kindersicherung die Aktivitäten Ihrer Kinder aufgezeichnet.

  Wenn Sie E-Mail-Benachrichtigungen erhalten möchten, gehen Sie wie folgt vor:

  1. Öffnen Sie das Dashboard der Kindersicherung über Ihr MyBitdefender-Konto.
  2. Klicken Sie auf das Symbol für **Allgemeine Einstellungen** in der rechten oberen Ecke.
  3. Aktivieren Sie die entsprechende Option, um Aktivitätsberichte zu erhalten.
  4. Geben Sie die Email-Adresse, an die Benachrichtigungen gesendet werden sollen, ein.
  5. Stellen Sie die Häufigkeit durch die Auswahl von täglich, wöchentlich oder monatlich ein.
  6. Sie erhalten E-Mail-Benachrichtigungen über:
     - Blockierte Websites
     - Blockierte Anwendungen
     - Blockierte IM-Kontakte
     - SMS von einem blockierten Kontakt
     - Eingegangene Anrufe von blockierten Telefonnummern
     - Entfernung der Facebook-Kindersicherungs-App
  7. Klicken Sie auf **Speichern**.

- Kontoinformationen

  Werfen Sie einen Blick auf die **Kontoinformationen**. Hier können Sie den Registrierungsstatus, den aktuellen Lizenzschlüssel und das Ablaufdatum einsehen.

- Aktivieren Sie die Option, um die auf Ihren Geräten installierten Agenten zu aktualisieren und das Update-Intervall festzulegen: täglich, wöchentlich oder monatlich.



Beachten Sie
Markieren Sie das entsprechende Kästchen, um den Willkommensbildschirm zu verbergen.

26.3. Konfigurieren der Kindersicherung

Im Dashboard der Kindersicherung können Sie sämtliche Module der Kindersicherung verwalten.

Jedes Modul enthält die folgenden Elemente: Name des Moduls, Statusmeldung, Symbol für das Modul und eine Schaltfläche , über die Sie wichtige Aufgaben in diesem Modul ausführen können.

Klicken Sie auf einen Reiter, um die entsprechenden Kindersicherungs-Funktionen für den Computer zu konfigurieren:

- Internet - Die Internetnutzung steuern und den Internet-Zugriff zeitliche begrenzen.
- Anwendungen - den Zugriff auf bestimmte Anwendungen blockieren oder beschränken.
- Facebook - Das Facebook-Konto Ihres Kindes schützen.
- Chat - Chat-Unterhaltungen mit bestimmten Kontakten zulassen oder blockieren.

Die folgenden Module stehen zur Überwachung der Aktivität Ihres Kindes auf seinem Mobilgerät zur Verfügung:

- Standort - den aktuellen Standort des Geräts Ihres Kindes in Google Maps anzeigen.
- SMS - Eingehende Textnachrichten von bestimmten Telefonnummern blockieren.
- Anrufe - Sowohl eingehende als auch ausgehende Anrufe von bestimmten Telefonnummern blockieren.

26.3.1. Web-Steuerung

Mit der Web-Steuerung können Sie Websites mit unangemessenen Inhalten blockieren und den Internetzugang zeitlich begrenzen.

So konfigurieren Sie die Web-Steuerung für ein bestimmtes Benutzerkonto:

1. Klicken Sie im Bereich **Web** auf , um das Fenster **Web-Aktivität** zu öffnen.
2. Über den Schalter können Sie die **Online-Aktivität** aktivieren.

Zulassen oder Blockieren einer Website

Im Fenster **Web-Aktivitäten** können Sie alle von Ihrem Kind aufgerufenen Webseiten einsehen.

- So können Sie den Zugriff auf eine bestimmte Website blockieren:
  1. Klicken Sie auf die Schaltfläche **Blacklist/Whitelist**.
  2. Geben Sie die Website in das entsprechende Feld ein.
  3. Klicken Sie auf **Blockieren**, um die Website zu der Liste hinzuzufügen.
  4. Wenn Sie sich später umentscheiden, wählen Sie einfach die Website aus und klicken Sie auf die entsprechende **Entfernen**-Schaltfläche.
- Um den Zugriff auf eine blockierte Website zu erlauben, gehen Sie folgendermaßen vor:
  1. Klicken Sie auf die Schaltfläche **Blacklist/Whitelist**.
  2. Geben Sie die Website in das entsprechende Feld ein.
  3. Klicken Sie auf **Zulassen**, um die Website zu der Liste hinzuzufügen.
  4. Wenn Sie sich später umentscheiden, wählen Sie einfach die Website aus und klicken Sie auf die entsprechende **Entfernen**-Schaltfläche.
- So können Sie den Zugriff auf eine Website nach Tageszeit festlegen:
  1. Öffnen Sie das Blacklist-/Whitelist-Web-Fenster, in dem die blockierten/zugelassenen Webseiten angezeigt werden.
  2. Klicken Sie unter dem Eintrag Berechtigung auf Blockiert (oder Zugelassen) und wählen Sie Planen aus dem Menü aus.
  3. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff erlaubt oder blockiert werden soll. Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren.

     Klicken Sie auf den Button **Speichern**.

Schlüsselwortsteuerung

Mit der Schlüsselwortsteuerung können Sie den Zugang zu Chat-Nachrichten und Webseiten blockieren, die bestimmte Wörter enthalten. Mit der Schlüsselwortsteuerung können Sie verhindern, dass Ihre Kinder unangemessene Wörter oder Sätze sehen, wenn sie im Internet sind. Zusätzlich können Sie sicher stellen dass sie keine persönlichen Daten (z.B. Adresse oder Telefonnummer) an Leute geben, die sie im Internet getroffen haben.

So können Sie die Schlüsselwortsteuerung für ein bestimmtes Benutzerkonto konfigurieren:

1. Klicken Sie auf die Schaltfläche **Schlüsselwörter**.
2. Geben Sie das Schlüsselwort in das entsprechende Feld ein.
3. Klicken Sie auf **Blockieren**, um das Wort zur Liste der unerlaubten Schlüsselwörter hinzuzufügen. Wenn Sie sich später umentscheiden, können Sie einfach auf die entsprechende **Entfernen**-Schaltfläche klicken.

Kategoriefilter

Der Kategoriefilter filtert den Zugriff auf Webseiten dynamisch anhand derer Inhalte. Wenn Sie das Alter Ihres Kindes angeben, wird der Kategoriefilter automatisch alle Website-Kategorien blockieren, die als unangemessen für diese Altersklasse gelten. Diese Konfiguration ist in den meisten Fällen ausreichend.

Wenn Sie die Inhalte, die Ihr Kind im Internet sieht, besser kontrollieren möchten, können Sie bestimmte Website-Kategorien auswählen, die vom Kategoriefilter blockiert werden sollen.

So können Sie die Einstellungen des Kategoriefilters im Detail anpassen:

1. Klicken Sie auf die Schaltfläche **Kategorien**.
2. Sie können nun überprüfen, welche Web-Kategorien für die aktuell ausgewählteAltersgruppe automatisch gesperrt/beschränkt werden. Wenn Sie mit den Standardeinstellungen nicht zufrieden sein sollten, können Sie diese nach Ihren Wünschen konfigurieren.
3. Klicken Sie auf **Speichern**. Wenn Sie sich später umentscheiden, klicken Sie auf **Zurücksetzen**, um den Standardschutz für die Altersklasse Ihres Kindes zu verwenden.

Zeitliche Beschränkung des Internet-Zugangs

Im Fenster **Web-Aktivität** finden Sie die **Planen**-Option, mit der Sie festlegen können, wann Ihr Kind auf das Internet zugreifen darf.

So können Sie den Zeitraum für die Internetnutzung für einen bestimmten Benutzer festlegen:

1. Klicken Sie auf die Schaltfläche **Zeitplan**.
2. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff blockiert sein soll. Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren.
3. Klicken Sie auf den Button **Speichern**.

26.3.2. Programmkontrolle

Mit der Anwendungssteuerung können Sie verhindern, dass bestimmte Programme ausgeführt werden. Sie können jede beliebige Anwendung sperren – neben Spiel-, Medien- und Chatprogrammen auch andere Arten von Software.

Um die Anwendungssteuerung für ein bestimmtes Benutzerkonto zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie im Bereich **Anwendungen** auf , um das Fenster **Anwendungsaktivität** zu öffnen.
2. Schalten Sie die **Anwendungsaktivität** mit dem Schalter ein.
3. Klicken Sie auf die Schaltfläche **Blacklist**.
4. Geben Sie den Namen der Anwendung ein:
   - Um eine Anwendung für ein Mobilgerät zu blockieren, wählen Sie die zu blockierenden Anwendung aus der Liste der **zugelassenen Anwendungen** aus.
   - Um eine Anwendung im Windows-Betriebssystem zu blockieren, fügen Sie die ausführbare Datei (.exe) der Anwendung, die Sie blockieren wollen, hinzu.
5. Klicken Sie auf **Blockieren**, um die Anwendung zur Liste der **blockierten Anwendungen** hinzuzufügen oder **Zulassen**, um sie zur Liste der **zugelassenen Anwendungen** hinzuzufügen.

26.3.3. Facebook-Schutz

Mit der Kindersicherung können Sie auch das Facebook-Konto Ihres Kindes überwachen und Berichte über die wichtigsten Aktivitäten dort erstellen.

Die Online-Aktivitäten werden geprüft, und eine Warnung wird ausgegeben, wenn sie eine Gefahr für Ihre Privatsphäre darstellen sollten.

Überwacht werden die folgenden Elemente:

- Anzahl der Freunde;
- Kommentare Ihres Kindes und seiner Freunde zu seinen Fotos und Beiträgen;
- Nachrichten
- Pinnwandbeiträge;
- hochgeladene Fotos und Videos;
- Privatsphäreneinstellungen des Kontos

So konfigurieren Sie den Facebook-Schutz für ein bestimmtes Benutzerkonto:

1. Klicken Sie im Bereich **Facebook** auf **Konto des Kindes verknüpfen**.
2. Installieren Sie über den entsprechenden Link die Anwendung, um das Facebook-Konto Ihres Kindes zu schützen.



Beachten Sie
Für die Installation der Anwendung benötigen Sie die Anmeldedaten für das Facebook-Profil Ihres Kindes.

Um die Überwachung des Facebook-Kontos zu beenden, klicken Sie oben auf die **Kontoverknüpfung aufheben**-Schaltfläche.

26.3.4. Chat-Steuerung

Mit der Chat-Steuerung können Sie die Chat-Kontakte überwachen und einschränken, mit denen Ihr Kind chattet. Sie können auch Chat-Nachrichten blockieren lassen, die bestimmte Wörter enthalten.



Beachten Sie
Die Chat-Steuerung ist nur für Yahoo! Messenger und Windows Live (MSN) Messenger verfügbar.

So können Sie die Chat-Steuerung für ein bestimmtes Benutzerkonto konfigurieren:

1. Klicken Sie im Bereich **Instant Messaging** auf , um das Fenster **Chat-Aktivität** zu öffnen.
2. Schalten Sie die **Chat-Aktivität** mit dem Schalter ein.

   Sie können die **Chat**-Aktivität über eine von zwei Optionen einschränken:

   - **Blacklist**-Schaltfläche zur Eingabe der E-Mail-Adresse, die zu dem Chat-Kontakt gehört.
   - über die Schaltfläche **Schlüsselwörter** - dies blockiert Chat-Nachrichten, die bestimmte Wörter enthalten.

26.3.5. Standort

Hier können Sie den aktuellen Gerätestandort in Google Maps anzeigen. Der Standort wird alle 5 Sekunden aktualisiert, eine Bewegung kann also nachverfolgt werden.

Die Genauigkeit der Ortung hängt davon ab, wie gut Bitdefender seinen Standort bestimmen kann:

- Wenn GPS im Gerät aktiviert ist, kann sein Standort bis auf ein paar Meter genau bestimmt werden, solange das Gerät in Reichweite der GPS-Satelliten (d. h. nicht in einem Gebäude) ist.
- Wenn sich das Gerät in einem Gebäude befindet, kann sein Standort auf mehrere zehn Meter genau bestimmt werden, solange WLAN aktiviert ist und Drahtlosnetzwerke in Reichweite des Geräts sind.
- Andernfalls wird der Standort allein über Daten aus dem Mobilfunknetzwerk bestimmt, wodurch die Genauigkeit auf einen Umkreis von ein paar hundert Metern sinkt.



Beachten Sie

Damit der **Standort** präzise bestimmt werden kann, sollten Sie sicherstellen, dass auf dem Mobilgerät GPS, WLAN oder die mobile Netzwerkverbindung aktiviert ist.

26.3.6. SMS-Steuerung

Mit der SMS-Steuerung können Sie den Empfang von Textnachrichten von bestimmten Telefonnummern verhindern.

- Um den Empfang von Textnachrichten von einer bestimmten Telefonnummer zu blockieren, gehen Sie folgendermaßen vor:

  1. Klicken Sie im Bereich **SMS** auf , um das Fenster **SMS-Aktivität** zu öffnen.
  2. Über den Schalter können Sie die **SMS-Aktivität** aktivieren.
  3. Klicken Sie auf die Schaltfläche **Blacklist**.
  4. Fügen Sie im entsprechenden Feld eine Telefonnummer hinzu.
  5. Klicken Sie auf **Blockieren**, um die Telefonnummer zur Blacklist hinzuzufügen. Die Nummer wird zur Liste der blockierten Telefonnummern hinzugefügt.

- Um den Empfang von Textnachrichten von einer blockierten Telefonnummer wieder zuzulassen, gehen Sie folgendermaßen vor:

  1. Klicken Sie oben auf die **Blacklist**-Schaltfläche.
  2. Wählen Sie die Telefonnummer aus der Liste aus.
  3. Klicken Sie auf **Entfernen**. Die Nummer wird aus der Liste der blockierten Telefonnummern entfernt.



Beachten Sie

Stellen Sie sicher, dass Sie die Länderkennung angeben, wenn Sie eine Telefonnummer in die Liste eintragen.

26.3.7. Telefonnummersteuerung

Mit der Telefonnummersteuerung können Sie ausgehende oder eingehende Anrufe von bestimmten Nummern verhindern.

- Um ausgehende oder eingehende Anrufe von bestimmten Telefonnummern zu blockieren, gehen Sie folgendermaßen vor:

  1. Klicken Sie im Bereich **Anrufe** auf , um das Fenster **Anruf-Aktivität** zu öffnen.
  2. Über den Schalter können Sie die **Anruf-Aktivität** aktivieren.
  3. Klicken Sie auf die Schaltfläche **Blacklist**.
  4. Fügen Sie im entsprechenden Feld eine Telefonnummer hinzu.

5. Klicken Sie auf **Blockieren**, um die Telefonnummer zur Blacklist hinzuzufügen. Die Nummer wird zur Liste der blockierten Telefonnummern hinzugefügt.

- Um Anrufe von einer blockierten Telefonnummer wieder zuzulassen, gehen Sie folgendermaßen vor:

1. Klicken Sie oben auf die **Blacklist**-Schaltfläche.
2. Wählen Sie die Telefonnummer aus der Liste aus.
3. Klicken Sie auf **Entfernen**. Die Nummer wird aus der Liste der blockierten Telefonnummern entfernt.



Beachten Sie

Stellen Sie sicher, dass Sie die Länderkennung angeben, wenn Sie eine Telefonnummer in die Liste eintragen.

27. SAFEGO FÜR FACEBOOK

Sie trauen Ihren Internet-Freunden, aber trauen Sie auch deren Computern? Nutzen Sie den Safego-Schutz für Facebook, um Ihr eigenes Benutzerkonto und das Ihrer Freunde vor Bedrohungen aus dem Internet zu schützen.

Safego ist eine Bitdefender-Anwendung zum Schutz Ihres Facebook-Kontos. Ihre Aufgabe besteht darin, die Links, die Sie von Ihren Freunden erhalten, zu scannen und die Privatsphäreeinstellungen Ihres Benutzerkontos zu überwachen.



Beachten Sie

Sie benötigen ein MyBitdefender-Konto, um diese Funktion nutzen zu können. Für weitere Informationen lesen Sie bitte *„MyBitdefender-Konto“* (S. 42).

Für Ihr Facebook-Konto stehen die folgenden Funktionen zur Verfügung:

- Scannt die Einträge in Ihren Neuigkeiten automatisch nach schädlichen Links.
- Schützt Ihr Konto vor Bedrohungen aus dem Internet.

  Wenn ein Beitrag oder Kommentar entdeckt wird, bei dem es sich um Spam, einen Phishing-Versuch oder eine Malware-Bedrohung handelt, erhalten Sie eine Warnmeldung.
- Warnt Ihre Freunde vor verdächtigen Links, die unter ihren Neuigkeiten eingestellt wurden.
- Hilft Ihnen dabei, ein sicheres Freundesnetzwerk mithilfe der **Friend-O-Meter**-Funktion aufzubauen.
- Überprüft den Status Ihrer Systemsicherheit mithilfe des Bitdefender-Quick Scan.

Um Safego für Facebook aufzurufen, gehen Sie folgendermaßen vor:

- Über die Bitdefender-Benutzeroberfläche:
  1. Öffnen Sie das Bitdefender-Fenster.
  2. Öffnen Sie den Bereich **Extras**.
  3. Wählen Sie im Modul **Safego Facebook-Schutz aktivieren** aus.

     Sie werden zu Ihrem Konto weitergeleitet.

4. Nutzen Sie Ihre Facebook-Anmeldeinformationen, um sich mit der Safego-Anwendung zu verbinden.
5. Erlauben Sie Safego, auf Ihr Facebook-Konto zuzugreifen.

Wenn Safego bereits aktiviert wurde, können Sie über **Berichte zu Facebook** im Menü Statistiken dazu einsehen.

- Über Ihr MyBitdefender-Konto:

1. Gehen Sie zu: https://my.bitdefender.com.
2. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Ihrem Konto an.
3. Klicken Sie auf **Facebook-Schutz**.

   Sie werden informiert, dass der Facebook-Schutz für Ihr Konto nicht aktiviert ist.
4. Klicken Sie auf **Aktivieren**, um fortzufahren.

   Sie werden zu Ihrem Konto weitergeleitet.
5. Nutzen Sie Ihre Facebook-Anmeldeinformationen, um sich mit der Safego-Anwendung zu verbinden.
6. Erlauben Sie Safego, auf Ihr Facebook-Konto zuzugreifen.

28. USB IMMUNIZER

Die Autostart-Funktion, die in jedem Windows-Betriebssystem angelegt ist, ist sehr praktisch, denn über sie kann der Computer direkt Dateien auf angeschlossenen Medien ausführen. So werden zum Beispiel eine Installation sofort gestartet, wenn die Installations-CD der Software eingelegt wird.

Leider kann Schad-Software diese Funktion missbrauchen, um sich automatisch von beschreibbaren Medien wie USB-Sticks und Speicherkarten aus auf Ihrem System einzunisten. In der letzten Zeit ist die Zahl der Angriffe über die Autostart-Funktion gewachsen.

Mit der USB-Immunisierung können Sie verhindern, dass mit NTFS, FAT32 oder FAT formatierte Flash-Speicher je wieder automatisch Malware ausführen. Wenn ein USB-Gerät einmal immunisiert wurde, kann es nicht mehr durch Malware dazu gebracht werden, eine bestimmte Anwendung auszuführen, sobald es mit einem Windows-Computer verbunden wird.

So können Sie ein USB-Gerät immunisieren:

1. Verbinden Sie das Flash-Laufwerk mit Ihrem Computer.
2. Suchen Sie das Gerät auf Ihrem Arbeitsplatz und klicken Sie mit der rechten Maustaste darauf.
3. Wählen Sie im Kontextmenü **Bitdefender** und anschließend **Dieses Laufwerk immunisieren**.



Beachten Sie

Wenn das Laufwerk bereits immunisiert wurde, wird anstatt der Immunisierungsoption folgende Meldung angezeigt: **Das USB-Gerät ist gegen Autostart-Malware geschützt.**

Sie können auch verhindern, dass Ihr Computer Malware von nicht immunisierten USB-Geräten startet, indem Sie die Autostart-Funktion deaktivieren. Für weitere Informationen lesen Sie bitte *„Automatische Schwachstellenüberwachung“* (S. 138).

29. FERNWARTUNG IHRER COMPUTER

Über Ihr MyBitdefender-Konto stehen Ihnen Fernwartungsfunktionen für die auf Ihren Computern installierten Bitdefender-Produkte zur Verfügung.

Über MyBitdefender können Sie auch aus der Ferne Aufgaben auf Ihren Computern erstellen und ausführen.

Jeder Computer kann über MyBitdefender verwaltet werden, sofern die folgenden Bedingungen erfüllt sind:

- Sie haben das Bitdefender Internet Security 2015-Produkt auf dem Computer installiert.
- Sie haben das Bitdefender-Produkt mit dem MyBitdefender-Konto verknüpft.
- Der Computer ist mit dem Internet verbunden.

29.1. MyBitdefender öffnen

Mit Bitdefender können Sie die Sicherheit Ihrer Computer verwalten, indem Sie in Ihren Bitdefender-Produkten Aufgaben erstellen.

Mit Bitdefender können Sie auf Ihr MyBitdefender-Konto von jedem Computer oder Mobilgerät mit Internetzugang aus zugreifen.

So öffnen Sie MyBitdefender:

- Von einem beliebigen Gerät mit Internetzugang aus:
  1. Öffnen Sie einen Web-Browser.
  2. Gehen Sie zu:https://my.bitdefender.com
  3. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Ihrem Konto an.
- Über Ihre Bitdefender-Benutzeroberfläche:
  1. Öffnen Sie das Bitdefender-Fenster.
  2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **MyBitdefender** aus dem Menü aus.

29.2. Aufgaben auf den Computern ausführen

Von Ihrem MyBitdefender-Konto aus können Sie Aufgaben auf Ihren Computern ausführen.

Wenn Sie unten im Fenster auf ein Computersybmol klicken, können Sie alle Verwaltungsaufgaben sehen, die Sie auf dem Remote-Computer ausführen können.

Produktregistrierung
Hier können Sie Bitdefender auf dem entfernten Rechner, durch Eingabe eines Lizenzschlüssels, registrieren.

Einen vollständigen Scan Ihres Computers durchführen
Hier können Sie einen entfernten Computer vollständig scannen.

Kritische Bereiche auf aktive Malware scannen
Hier können Sie einen Quick-Scan auf dem entfernten Computer durchführen.

Kritische Probleme beheben
Hier können Sie die Probleme beheben, die auf dem entfernten Computer aufgetreten sind.

Produkt-Update
Startet den Update-Vorgang für das auf diesem Computer installierte Bitdefender-Produkt.

SYSTEMOPTIMIERUNG

30. PC-TUNING

Bitdefender enthält ein PC-Tuning-Modul, das Ihnen hilft, die Unversehrtheit Ihres Systems zu bewahren. Die Wartungsprogramme sind wichtig für die Verbesserung der Reaktionszeit Ihres Systems und die effiziente Verwaltung des Festplattenspeichers.

Bitdefender bietet die folgenden PC-Tuning-Tools:

- Die Ein-Klick-Optimierung analysiert und verbessert Ihre Systemgeschwindigkeit, indem es mit nur einem Klick eine Vielzahl von Aufgaben ausführt.
- Die Systemstartoptimierung verhindert, dass beim Systemstart nicht benötigte Anwendungen ausgeführt werden, um die Startzeit zu verkürzen.
- PC Clean-Up entfernt temporäre Internet-Dateien und Cookies, ungenutzte Systemdateien und kürzlich verwendete Dokumentverknüpfungen.
- Festplatten-Defragmentierer reorganisiert die Daten auf der Festplatte, so dass die Teile einer Datei nah beieinander gespeichert werden.
- Die Registry-Bereinigung erkennt und löscht ungültige oder verwaiste Referenzen in der Windows-Registry. Um die Windows-Registry sauber und optimiert zu halten, wird empfohlen die Registry-Bereinigung einmal im Monat durchzuführen.
- Registry-Wiederherstellung kann die zuvor durch die Bitdefender-Registry-Bereinigung gelöschten Lizenzschlüssel der Windows-Registry wiederherstellen.
- Der Dublettenfinder findet und löscht doppelte Dateien auf Ihrem System.

30.1. Optimierung der Systemgeschwindigkeit mit nur einem Klick

Probleme wie Festplattenausfälle, nicht mehr benötigte Registry-Dateien und Browser-Verläufe können Ihren Computer ausbremsen und äußerst lästig werden. All diese Probleme können mit nur einem Klick behoben werden.

Die Ein-Klick-Optimierung ermöglicht das Auffinden und die Entfernung von nicht mehr benötigten Dateien, indem es eine Vielzahl von Bereinigungsaufgaben gleichzeitig ausführt.

So können Sie die Ein-Klick-Optimierung starten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie im Modul **PC-Tuning** auf **Ein-Klick-Optimierung**. Klicken Sie zum Verlassen auf **Abbrechen**.
   a. **Analyse**

      Bitte warten Sie, bis Bitdefender die Suche nach Systemproblemen abgeschlossen hat.

      - Datenträgerbereinigung - Findet alte und nicht mehr benötigte Systemdateien.
      - Registry-Bereinigung - Findet ungültige oder verwaiste Referenzen in der Windows-Registry.
      - Datenschutz-Bereinigung - Findet temporäre Internet-Dateien und Cookies sowie Browser-Cache und -Verlauf.

      Die Anzahl der gefundenen Probleme wird angezeigt. Diese sollten erneut überprüft werden, bevor Sie mit dem Bereinigungsprozess fortfahren. Klicken Sie zum Fortfahren auf **Optimieren**.

   b. **Systemoptimierung**

      Bitte warten Sie, bis Bitdefender die Systemoptimierung abgeschlossen hat.

   c. **Probleme**

      Hier können Sie das Ergebnis der Operation sehen.

      Klicken Sie auf den Link **Ausführlichen Bericht zeigen**, um umfassende Informationen zum Optimierungsprozess zu erhalten.

30.2. Optimieren der Systemstartzeit

Eine zu lange Systemstartzeit wird durch Anwendungen verursacht, die unnötigerweise ausgeführt werden, und kann zu einem echten Problem werden. Minutenlanges Warten auf den Systemstart kostet Sie wertvolle Zeit und beeinträchtigt Ihre Produktivität.

Im Fenster der Systemstartoptimierung werden alle Anwendungen angezeigt, die beim Systemstart ausgeführt werden. Hier können Sie auch ihr Verhalten festlegen.

So können Sie die Systemstartoptimierung starten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie im Modul **PC-Tuning** auf **Systemstartoptimierung**.

   a. **Anwendungen auswählen**

      Hier sehen Sie eine Liste der Anwendungen, die beim Systemstart ausgeführt werden. Wählen Sie die Anwendungen aus, die Sie deaktivieren oder beim Systemstart verzögern wollen.

   b. **Auswahl anderer Nutzer**

      Erfahren Sie, welche Auswahl andere Bitdefender-Benutzer für die ausgewählte Anwendung getroffen haben. Je nach Programmverwendung werden drei Stufen angezeigt: **Hoch**, **Mittel** und **Gering**.

   c. **Systemstartzeit**

      Überprüfen Sie den Regler oben im Fenster, um die Zeit anzuzeigen, die Ihr System und die ausgewählten Anwendungen beim Start benötigen.

      Ein Systemneustart ist erforderlich, um die Informationen zur Startzeit von System und Anwendungen einzuholen.

   d. **Systemstart-Status**

      - **Aktivieren.** Wählen Sie diese Option aus, wenn eine Anwendung beim Systemstart ausgeführt werden soll. Die Option ist standardmäßig aktiviert.
      - **Verzögern.**

        Wählen Sie diese Option aus, um die Programmausführung beim Systemstart zu verschieben. Das bedeutet, dass die ausgewählten Anwendungen nach der Anmeldung des Benutzers am System mit einer fünfminütigen Verzögerung gestartet werden.
        Die **Verzögern**-Funktion ist vordefiniert und kann nicht vom Benutzer konfiguriert werden.
      - **Deaktivieren.** Wählen Sie diese Option aus, um die Programmausführung beim Systemstart zu deaktivieren.

   e. **Bericht**

Informationen wie die geschätzte Systemstartzeit nach Verzögerung oder Deaktivierung von Programmen wird angezeigt.

Das System muss eventuell neu gestartet werden, um alle Informationen anzuzeigen.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.



Beachten Sie

Falls Ihre Lizenz ausläuft oder Sie sich entscheiden, Bitdefender zu deinstallieren, werden die Starteinstellungen für die Programme, die Sie von der Ausführung beim Systemstart ausgenommen haben, auf den Standard zurückgesetzt.

30.3. Bereinigen Ihres PCs

Bei jedem Besuch einer Webseite werden temporäre Internet-Dateien auf Ihrer Festplatte abgelegt, um den Zugriff beim nächsten Mal zu beschleunigen.

Cookies werden ebenfalls auf Ihrem Computer gespeichert wenn Sie eine Webseite besuchen.

Der PC-Clean-Up-Assistent hilft Ihnen, Speicherplatz auf der Festplatte zu gewinnen und Ihre Privatsphäre zu schützen, indem er Dateien löscht, die nicht mehr benötigt werden.

- Browser-Cache (Internet Explorer, Mozilla Firefox, Google Chrome).
- Debugging-Informationen (Fehlerberichterstattungsdateien, Speicherabbilder und Protokolle, die im Windows-Betrieb erstellt werden).
- Windows-Junk-Dateien (Papierkorb und temporäre Systemdateien).

Um den PC-Clean-Up-Assistenten zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Wählen Sie im Bereich **PC-Tuning PC-Bereinigung** aus.
4. Folgen Sie der dreiteiligen Anleitung, um eine Bereinigung durchzuführen. Über die Schaltfläche **Weiter** können Sie im Assistenten blättern. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

   a. **Willkommen**

Wählen Sie **Typisch** oder **Benutzerdefiniert**. Klicken Sie auf **Weiter**, um fortzufahren.

b. **Bereinigung durchführen**

c. **Bericht**

30.4. Defragmentieren der Festplattenlaufwerke

Wenn eine Datei mehr Speicher als der größte Block freien Speichers benötigt, werden Daten fragmentiert. Da der Speicherblock nicht ausreicht, die Datei in einem Stück zu speichern, wird die Datei über die freien Blöcke der Festplatte verteilt. Beim Zugriff auf die Datei muss sie dann von verschiedenen Stellen der Festplatte gelesen werden.

Es wird empfohlen, die Festplatte zu defragmentieren, um:

- Dateizugriffe zu beschleunigen.
- die generelle Systemgeschwindigkeit zu verbessern.
- die Lebensdauer der Festplatte zu erhöhen.

Um den Defragmentierungsassistenten zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras.**
3. Wählen Sie im Bereich **PC-Tuning Defragmentierung** aus.
4. Folgen Sie der fünfteiligen Anleitung, um eine Defragmentierung durchzuführen. Über die Schaltfläche **Weiter** können Sie im Assistenten blättern. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

a. **Zur Analyse auswählen**

Wählen Sie die Partitionen, die fragmentiert werden sollen, aus. Klicken Sie auf **Fortfahren**, um den Analyseprozess zu starten.

b. **Analyse**

Warten Sie, bis Bitdefender die Analyse der Partitionen abgeschlossen hat.

c. **Zur Defragmentierung auswählen**

Der Fragmentierstatus der analysierten Partitionen wird angezeigt. Wählen Sie die Partitionen, die defragmentiert werden sollen.

d. **Defrag-mentierung**

Warten Sie, bis Bitdefender die Defragmentierung der Partitionen abgeschlossen hat.

e. **Bericht**



Beachten Sie

Die Defragmentierung kann einige Zeit in Anspruch nehmen, da Daten über die komplette Festplatte verschoben werden. Wir empfehlen deshalb die Defragmentierung durchzuführen, wenn Sie den Computer gerade nicht verwenden.

30.5. Bereinigen der Windows-Registry

Viele Anwendungen legen während der Installation Schlüssel in der Windows-Registry an. Wenn diese Software dann wieder deinstalliert wird, bleiben häufig einige Schlüssel in der Registry zurück. Dies führt zur Verlangsamung und evtl. sogar zur Instabilität des Systems. Dasselbe kann passieren, wenn Sie Verknüpfungen oder einzelne Dateien einer Anwendung löschen oder wenn defekte Treiber vorliegen.

Um den Assistenten für die Registry-Bereinigung zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras.**
3. Wählen Sie im Bereich **PC-Tuning Registry-Bereinigung** aus.
4. Folgen Sie der vierteiligen Anleitung, um die Registry zu bereinigen. Über die Schaltfläche **Weiter** können Sie im Assistenten blättern. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

   a. **Willkommen**

   b. **Scan durchführen**

   Bitte warten Sie, bis Bitdefender den Registry-Scan abgeschlossen hat.

   c. **Schlüssel auswählen**

   Hier werden alle gefundenen ungültigen oder verwaisten Registry-Schlüssel angezeigt. Für jeden Registry-Schlüssel stehen detaillierte Informationen zur Verfügung (Name, Wert, Priorität, Kategorie).

Die Registry-Schlüssel sind entsprechend ihrer Position in der Windows-Registry gruppiert:

- **Software-Speicherorte.** Registry-Schlüssel, die Informationen über den Pfad zu Anwendungen auf Ihrem Computer enthalten.

  Ungültigen Schlüsseln wird eine niedrige Priorität zugewiesen, was bedeutet, dass Sie diese nahezu ohne Risiko löschen können.

- **Benutzerdefinierte Steuerungen.** Registry-Schlüssel die Informationen über die Endungen, die auf Ihrem Computer registriert sind, enthalten. Diese Registry-Schlüssel werden verwendet, um Dateizuordnungen zu verwalten (um sicherzustellen, dass das richtige Programm geöffnet wird, wenn Sie über den Windows Explorer eine Datei öffnen). So erlaubt solch ein Registry-Schlüssel beispielsweise, dass Windows eine Datei mit der Endung .doc in Microsoft Word öffnet.

  Ungültigen Schlüsseln wird eine niedrige Priorität zugewiesen, was bedeutet, dass Sie diese nahezu ohne Risiko löschen können.

- **Gemeinsam genutzte DLLs.** Registry-Schlüssel, die Informationen über die Position von DLLs (Dynamic Link Libraries) enthalten. DLLs speichern Funktionen, die von installierten Anwendungen verwendet werden, um bestimmte Aufgaben auszuführen. Diese können von verschiedenen Anwendungen gemeinsam gentutzt werden, um den benötigten Speicherplatz so gering wie möglich zu halten.

  Diese Registry-Schlüssel werden ungültig, wenn die entsprechende DLL in eine andere Position verschoben oder komplett entfernt wird (dies passiert wenn Sie ein Programm deinstallieren).

  Den ungültigen Schlüsseln wird eine mittlere Priorität zugewiesen, was bedeutet dass ein Löschen negative Auswirkungen auf das System haben kann.

In der Voreinstellung werden alle Schlüssel für eine Löschung markiert. Sie können einzelne ungültige Schlüssel aus einer markierten Kategorie zu löschen.

d. **Bericht**

30.6. Wiederherstellen der bereinigten Registry

Manchmal kann es vorkommen, dass nach einer Bereinigung der Registry das System nicht mehr fehlerfrei arbeitet oder manche Anwendungen wegen

der fehlenden Schlüssel nicht mehr funktionieren. Das kann passieren, wenn Registry-Schlüssel, die von mehreren Programmen genutzt wurden, bei der Bereinigung oder auf anderem Wege gelöscht wurden. Um ein solches Problem zu beheben, müssen Sie die fehlenden Registry-Schlüssel wiederherstellen.

Um den Assistenten für die Registry-Wiederherstellung zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras.**
3. Wählen Sie im Bereich **Tune-Up Registry-Wiederherstellung** aus.
4. Folgen Sie der zweistufigen Anleitung, um die bereinigte Registry wiederherzustellen. Über die Schaltfläche **Weiter** können Sie im Assistenten blättern. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

   a. **Herstellungspkt. wählen**

      Hier können Sie sehen, zu welchen Zeitpunkten die Windows-Registry bereinigt wurde. Klicken Sie auf den Link **Datei anzeigen**, um die gefundenen Registry-Schlüssel anzuzeigen. Wählen Sie den Zeitpunkt aus, zu dem die Windows-Registry wiederhergestellt werden soll.

      Warnung
      Die Wiederherstellung der bereinigten Registry kann dazu führen, dass existierende Schlüssel überschrieben werden, die seit der letzten Bereinigung geändert wurden.

   b. **Ergebnisse**

30.7. Auffinden von Dubletten

Doppelte Dateien (Dubletten) verschwenden Speicherplatz. Denken Sie z.B. an identische MP3-Dateien in drei verschiedenen Ordnern.

Der Assistent zur Dublettensuche hilft Ihnen, Dubletten auf Ihrem Computer zu finden und zu löschen.

Um den Assistenten für die Dublettensuche zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.

2. Öffnen Sie den Bereich **Extras.**
3. Wählen Sie im Bereich **PC-Tuning Dublettensuche** aus.
4. Folgen Sie der vierteiligen Anleitung, um Dubletten zu finden und zu entfernen. Über die Schaltfläche **Weiter** können Sie im Assistenten blättern. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

   a. **Ziel auswählen**

      Fügen Sie die Verzeichnisse, in denen nach Dubletten gesucht werden soll, hinzu.

   b. **Dubletten suchen**

      Bitte warten Sie, bis Bitdefender die Suche nach Dubletten abgeschlossen hat.

   c. **Zu löschende Dateien**

      Identische Dateien sind in Gruppen aufgelistet. Sie können wählen, ob eine Aktion für alle Gruppen oder jede Gruppe separat angewendet wird: die neueste behalten, die älteste behalten oder keine Aktion ausführen. Sie können auch für jede individuelle Datei eine Aktion auswählen.

      Beachten Sie

      Werden keine Dubletten gefunden, wird dieser Schritt übersprungen.

   d. **Bericht**

31. PROFILE

Das Arbeiten, Filme schauen oder Spielen am Computer kann das System verlangsamen, ganz besonders dann, wenn diese Aktivitäten mit Windows-Update-Vorgängen oder Wartungsaufgaben einhergehen. Mit Bitdefender können Sie jetzt ein bevorzugtes Profil auswählen und anwenden und damit Ihr System so anpassen, dass die jeweils benötigten Anwendungen optimal laufen.

Bitdefender bietet die folgenden Profile:

- Arbeitsprofil
- Filmprofil
- Spielprofil

Falls Sie sich entscheiden, die **Profile** nicht zu nutzen, wird ein voreingestelltes Profil mit dem Namen **Standard** aktiviert, dass Ihr System nicht optimiert.

In Übereinstimmung mit Ihrer Aktivität werden die folgenden Produkteinstellungen vorgenommen, wenn ein Profil aktiviert wird:

- Alle Bitdefender-Alarme und Pop-ups sind deaktiviert.
- Automatische Updates werden verschoben.
- Geplante Scans werden verschoben.
- Der Suchberater wird deaktiviert.
- Die Sicherheitsstufe der Angriffserkennung ist auf **Tolerant** gesetzt.
- Benachrichtigungen zu Sonderangeboten und Produktbenachrichtigungen sind deaktiviert.

In Übereinstimmung mit Ihrer Aktivität werden die folgenden Systemeinstellungen vorgenommen, wenn ein Profil aktiviert wird:

- Automatische Windows-Updates werden verschoben.
- Windows-Benachrichtigungen und Pop-ups sind deaktiviert.
- Nicht benötigte Hintergrundprogramme werden angehalten.
- Die visuellen Effekte werden für maximale Leistung optimiert.
- Wartungsaufgaben werden verschoben.

- Die Energiespareinstellungen werden angepasst.

31.1. Arbeitsprofil

Das gleichzeitige Ausführen von verschiedenen Aufgaben bei der Arbeit am PC, so zum Beispiel das Versenden von E-Mails, das Abhalten von Videokonferenzen mit Kollegen oder das Arbeiten mit Grafikprogrammen, können die Leistung Ihres Systems beeinträchtigen. Das Arbeitsprofil wurde entwickelt, um Sie effizienter arbeiten zu lassen. Dafür werden einige Hintergrunddienste und Wartungsaufgaben deaktiviert.

Konfigurieren des Arbeitsprofils

So konfigurieren Sie die durchzuführenden Aktionen für das Arbeitsprofil:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Klicken Sie im Fenster **Profileinstellungen** auf die **Konfigurieren**-Schaltfläche im Bereich Arbeitsprofil.
5. Wählen Sie die Systemanpassungen aus, die Sie durchführen möchten, indem Sie die folgenden Optionen auswählen:
   - Die Systemleistung für Arbeitsanwendungen steigern
   - Produkteinstellungen für das Arbeitsprofil optimieren
   - Hintergrundprogramme und Wartungsaufgaben verschieben
   - Automatische Windows-Updates später durchführen
6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Manuelles Hinzufügen von Anwendungen zur Arbeitsprofilliste

Wenn das Arbeitsprofil im Bitdefender beim Aufrufen einer Arbeitsanwendung nicht automatisch aktiviert wird, können Sie die Anwendung manuell zu der **Anwendungsliste** hinzufügen.

So fügen Sie Anwendungen manuell zur Anwendungsliste im Arbeitsprofil hinzu:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Klicken Sie im Fenster **Profile** auf die **Konfigurieren**-Schaltfläche im Bereich Arbeitsprofil.
5. Klicken Sie im Fenster **Arbeitsprofil** auf den Link zur **Anwendungsliste**.
6. Klicken Sie auf **Hinzufügen**, um eine neue Anwendung zur **Anwendungsliste** hinzuzufügen.

   Ein neues Fenster wird sich öffnen. Scrollen Sie bitte bis zu der ausführbaren Datei der Anwendung, wählen Sie diese aus und klicken Sie auf **OK**, um diese zu der Liste hinzuzufügen.

31.2. Filmprofil

Das Abspielen von Videos mit hoher Qualität, so zum Beispiel HD-Filme, nimmt viele Systemressourcen in Anspruch. Mit dem Filmprofil werden die System- und Produkteinstellungen so angepasst, dass Sie Ihre Filme ungestört genießen können.

Konfigurieren des Filmprofils

So konfigurieren Sie die durchzuführenden Aktionen für das Filmprofil:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Klicken Sie im Fenster **Profileinstellungen** auf die **Konfigurieren**-Schaltfläche im Bereich Filmprofil.
5. Wählen Sie die Systemanpassungen aus, die Sie durchführen möchten, indem Sie die folgenden Optionen auswählen:
   - Die Systemleistung für das Abspielen von Videos steigern
   - Produkteinstellungen für das Filmprofil optimieren
   - Hintergrundprogramme und Wartungsaufgaben verschieben
   - Automatische Windows-Updates später durchführen

- Energiesparplan und visuelle Einstellungen für Filme anpassen

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Manuelles Hinzufügen von Video-Playern zur Filmprofilliste

Wenn das Filmprofil im Bitdefender beim Aufrufen eines Video-Players nicht automatisch aktiviert wird, können Sie den Player manuell zu der **Player-Liste** hinzufügen.

So fügen Sie Video-Player manuell zur Player-Liste im Filmprofil hinzu:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Klicken Sie im Fenster **Profileinstellungen** auf die **Konfigurieren**-Schaltfläche im Bereich Filmprofil.
5. Klicken Sie im Fenster **Filmprofil** auf den Link zur **Player-Liste**.
6. Klicken Sie auf **Hinzufügen**, um einen neuen Player zur **Player-Liste** hinzuzufügen.

   Ein neues Fenster wird sich öffnen. Scrollen Sie bitte bis zu der ausführbaren Datei der Anwendung, wählen Sie diese aus und klicken Sie auf **OK**, um diese zu der Liste hinzuzufügen.

31.3. Spielprofil

Um Ihre Spiele ohne Unterbrechungen genießen zu können, müssen Systemunterbrechungen und Leistungseinbußen unbedingt minimiert werden. Durch die Kombination von verhaltensbasierten Heuristiken und einer Liste bekannter Spiele kann Bitdefender automatisch erkennen, ob ein Spiel ausgeführt wird, und Ihre Systemressourcen so optimieren, dass Sie in Ruhe spielen können.

Konfigurieren des Spielprofils

So konfigurieren Sie die durchzuführenden Aktionen für das Spielprofil:

1. Öffnen Sie das Bitdefender-Fenster.

2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Klicken Sie im Fenster **Profileinstellungen** auf die **Konfigurieren**-Schaltfläche im Bereich Spielprofil.
5. Wählen Sie die Systemanpassungen aus, die Sie durchführen möchten, indem Sie die folgenden Optionen auswählen:
   - Die Systemleistung für Spiele steigern
   - Produkteinstellungen für das Spielprofil optimieren
   - Hintergrundprogramme und Wartungsaufgaben verschieben
   - Automatische Windows-Updates später durchführen
   - Energiesparplan und visuelle Einstellungen für Spiele anpassen
6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Spiele manuell zu der Spielliste hinzufügen

Wenn das Spielprofil im Bitdefender beim Aufrufen eines Spiels oder einer Anwendung nicht automatisch aktiviert wird, können Sie die Anwendung manuell zu der **Spieleliste** hinzufügen.

So fügen Sie Spiele manuell zur Spieleliste im Spielprofil hinzu:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Klicken Sie im Fenster **Profileinstellungen** auf die **Konfigurieren**-Schaltfläche im Bereich Spielprofil.
5. Klicken Sie im Fenster **Spielprofil** auf den Link zur **Spieleliste**.
6. Klicken Sie auf **Hinzufügen**, um ein neues Spiel zur **Spieleliste** hinzuzufügen.

   Ein neues Fenster wird sich öffnen. Öffnen Sie den Ordner, in dem sich die ausführbare Datei des Spiels befindet, markieren Sie sie und klicken Sie auf **OK**, um das Spiel zur Liste hinzuzufügen.

31.4. Echtzeitoptimierung

Die Bitdefender-Echtzeitoptimierung ist ein Plug-in, das Ihre Systemleistung unbemerkt im Hintergrund verbessert und so sicherstellt, dass Sie im Profile-Modus nicht gestört werden. Je nach CPU-Auslastung überwacht das Plug-in alle Prozesse und konzentriert sich dabei auf Prozesse, die Ihr System überdurchschnittlich belasten, um sie an Ihre Anforderungen anzupassen.

So können Sie die Echtzeitoptimierung aktivieren oder deaktivieren:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen Sie den Bereich **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Wählen Sie im Fenster **Profile** den Reiter **Profileinstellungen** aus.
5. Aktivieren oder deaktivieren Sie die Echtzeitoptimierung, indem Sie auf den entsprechenden Schalter klicken.

PROBLEMLÖSUNG

32. VERBREITETE PROBLEME BEHEBEN

In diesem Kapitel werden einige Probleme, die Ihnen bei der Verwendung von Bitdefender begegnen können, erläutert. Zudem finden Sie hier Lösungsvorschläge für diese Probleme. Die meisten dieser Probleme können über eine passende Konfiguration der Produkteinstellungen gelöst werden.

- *„Mein System scheint langsamer zu sein“* (S. 199)
- *„Der Scan startet nicht“* (S. 201)
- *„Ich kann eine Anwendung nicht mehr ausführen“* (S. 204)
- *„Wie gehe ich vor, wenn Bitdefender eine sichere Website oder Online-Anwendung blockiert?“* (S. 205)
- *„Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann“* (S. 210)
- *„Mein Computer ist nicht mit dem Internet verbunden. Wie kann ich Bitdefender aktualisieren?“* (S. 211)
- *„Bitdefender-Dienste antworten nicht“* (S. 211)
- *„Der Spam-Schutz-Filter funktioniert nicht richtig“* (S. 212)
- *„Das automatische Einfügen funktioniert bei meiner Geldbörse nicht“* (S. 217)
- *„Entfernen von Bitdefender ist fehlgeschlagen“* (S. 219)
- *„Mein System fährt nach der Installation von Bitdefender nicht mehr hoch“* (S. 221)

Wenn Sie Ihr Problem hier nicht finden oder wenn die vorgeschlagene Lösung nicht zum Erfolg führt, können Sie den technischen Kundendienst von Bitdefender wie in Kapitel *„Hilfe anfordern“* (S. 238) beschrieben, kontaktieren.

32.1. Mein System scheint langsamer zu sein

Nach der Installation einer Sicherheitssoftware ist eine geringfügige Verlangsamung des Systems bis zu einem gewissen Grad normal.

Wenn Sie eine erhebliche Systemverlangsamung feststellen, kann dies folgende Ursachen haben:

- **Bitdefender ist nicht die einzige auf Ihrem System installierte Sicherheits-Software.**

Obwohl Bitdefender bereits auf Ihrem System installierte Sicherheitsprogramme während der Installation sucht und entfernt, empfehlen wir dennoch, jedes andere Virenschutzprogramm von Ihrem Rechner zu entfernen, bevor Sie die Installation von Bitdefender starten. Für weitere Informationen lesen Sie bitte *„Wie entferne ich andere Sicherheitslösungen?“* (S. 86).

- **Die Mindestsystemanforderungen für die Ausführung von Bitdefender sind nicht erfüllt.**

  Wenn Ihr PC die Mindestsystemanforderungen nicht erfüllt, verlangsamt dies Ihr System, insbesondere dann, wenn mehrere Anwendungen gleichzeitig laufen. Für weitere Informationen lesen Sie bitte *„Mindestsystemanforderungen“* (S. 3).

- **In Ihrer Windows-Registry befinden sich zu viele ungültige Registry-Schlüssel.**

  Die Bereinigung der Windows-Registry kann die Leistung Ihres Systems verbessern. Für weitere Informationen lesen Sie bitte *„Bereinigen der Windows-Registry“* (S. 188).

- **Ihre Festplatte ist zu fragmentiert.**

  Dateifragmentierung verzögert den Zugriff auf Dateien und verschlechtert die Systemleistung.

  Durch die Ausführung des Festplattendefragmentierers kann sich die Leistung Ihres Systems verbessern. Für weitere Informationen lesen Sie bitte *„Defragmentieren der Festplattenlaufwerke“* (S. 187).

  Um Ihre Festplatte mithilfe Ihres Windows-Betriebssystems zu defragmentieren, folgen Sie diesem Pfad vom Windows-Startmenü aus: **Start** → **Alle Programme** → **Zubehör** → **Systemprogramme** → **Defragmentierung**.

- **Sie haben Anwendungen auf Ihrem Computer, die Sie nicht nutzen**.

  Auf jedem Computer befinden sich Programme oder Anwendungen, die Sie nicht benutzen. Im Hintergrund laufen viele unerwünschte Programme, die Speicherplatz und Arbeitsspeicher beanspruchen. Wenn Sie ein Programm nicht nutzen, deinstallieren Sie es. Das gilt auch für vorinstallierte Software oder Testversionen, die Sie nicht wieder entfernt haben.



Wichtig

Wenn Sie glauben, dass ein Programm oder eine Anwendung ein wichtiger Bestandteil Ihres Betriebssystems ist, entfernen Sie es nicht und wenden Sie sich an den Bitdefender-Kundendienst.

- **Ihr System ist vielleicht infiziert.**

  Die Geschwindigkeit und das allgemeine Verhalten Ihres Systems kann auch durch Malware beeinträchtigt werden. Spyware, Viren, Trojaner und Adware wirken sich negativ auf Ihre Systemleistung aus. Stellen Sie sicher, dass Ihr System regelmäßig gescannt wird, mindestens einmal pro Woche. Es empfiehlt sich, einen Bitdefender-System-Scan durchzuführen, da so nach allen Malware-Typen gesucht wird, die die Sicherheit Ihres Systems bedrohen.

  Um den System-Scan zu starten, gehen Sie folgendermaßen vor:

  1. Öffnen Sie das Bitdefender-Fenster.
  2. Öffnen die den Bereich **Schutz**.
  3. Wählen Sie im Modul **Virenschutz System-Scan** aus.
  4. Befolgen Sie die Anweisungen des Assistenten.

32.2. Der Scan startet nicht

Dieses Problem kann folgende Ursachen haben:

- **Eine vorherige Installation von Bitdefender wurde nicht vollständig entfernt oder es handelt sich um eine fehlerhafte Bitdefender-Installation.**

  Befolgen Sie dafür die folgenden Schritte:

  1. Entfernen Sie Bitdefender vollständig von Ihrem System:
     - In **Windows XP**:
       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme hinzufügen/entfernen**.
       b. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Entfernen**.
       c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- Für **Windows Vista** und **Windows 7**:

  a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.

  b. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.

  c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

  d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- In **Windows 8**:

  a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

  b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

  c. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.

  d. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

  e. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

2. Installieren Sie Ihr Bitdefender-Produkt erneut.

- **Bitdefender ist nicht die einzige auf Ihrem System installierte Sicherheits-Software**.

  Befolgen Sie dafür die folgenden Schritte:

  1. Entfernen Sie die andere Sicherheitslösung. Für weitere Informationen lesen Sie bitte *„Wie entferne ich andere Sicherheitslösungen?“* (S. 86).

  2. Entfernen Sie Bitdefender vollständig von Ihrem System:

     - In **Windows XP**:

a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme hinzufügen/entfernen**.

b. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Entfernen**.

c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- Für **Windows Vista** und **Windows 7**:

a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.

b. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.

c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- In **Windows 8**:

a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

c. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.

d. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

e. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

3. Installieren Sie Ihr Bitdefender-Produkt erneut.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

32.3. Ich kann eine Anwendung nicht mehr ausführen

Dieses Problem tritt auf, wenn Sie versuchen, ein Programm zu verwenden, das vor der Installation von Bitdefender einwandfrei funktioniert hatte.

Nach der Installation von Bitdefender könnten folgende Situationen eintreten:

- Sie könnten einen Benachrichtigung von Bitdefender erhalten, dass das Programm versucht, Veränderungen am System durchzuführen.
- Es ist möglich, dass Sie von dem Programm, das Sie starten möchten, eine Fehlermeldung erhalten.

Diese Situation tritt ein, wenn Active Virus Control eine Anwendung fälschlicherweise als Malware einstuft.

Active Virus Control ist ein Bitdefender-Modul, das ständig die laufenden Programme Ihres Systems überwacht und einen Bericht über jene sendet, die sich potenziell gefährlich verhalten. Da diese Funktion auf dem heuristischen System basiert, kann es Fälle geben, in denen einwandfreie Anwendungen im Bericht der Active Virus Control aufgelistet werden.

Wenn diese Situation eintritt, können Sie die entsprechende Anwendung von der Überwachung durch Active Virus Control ausschließen.

Wenn Sie das Programm der Ausschlussliste hinzufügen möchten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Ausschlüsse** aus.
5. Klicken Sie auf den Link **Ausgeschlossene Prozesse**. Ein Fenster wird angezeigt. Hier können Sie die Prozesse verwalten, die von Active Virus Control ausgeschlossen sind.
6. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
   b. Klicken Sie auf **Durchsuchen**, wählen Sie die Anwendung, die ausgeschlossen werden soll und klicken Sie dann auf **OK**.
   c. Lassen Sie die **Zulassen**-Option aktiviert, um zu verhindern, dass Active Virus Control die Anwendung blockiert.

d. Klicken Sie auf **Hinzufügen**.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

32.4. Wie gehe ich vor, wenn Bitdefender eine sichere Website oder Online-Anwendung blockiert?

Bitdefender ermöglicht Ihnen sicheres Surfen im Netz, indem es den Internet-Datenverkehr filtert und schädliche Inhalte blockiert. Es kann jedoch auch vorkommen, dass Bitdefender eine sichere Website oder Online-Anwendung als unsicher einstuft, wodurch diese dann durch den Bitdefender-Scan des HTTP-Datenverkehrs irrtümlich blockiert werden.

Sollte die gleiche Seite oder Anwendung wiederholt blockiert werden, können Sie diese zu einer sogenannten Whitelist hinzufügen, damit sie von den Bitdefender-Engines nicht mehr gescannt werden. So können Sie ungestört im Internet surfen.

So fügen Sie eine Website zur **Whitelist** hinzu:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Internet-Schutz**.
4. Klicken Sie im Reiter **Einstellungen** auf den Link **Whitelist**. Ein neues Fenster wird sich öffnen.
5. Geben Sie die Adresse der blockierten Website oder Online-Anwendung in das entsprechende Feld ein und klicken Sie **Hinzufügen**.
6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Sie sollten dieser Liste nur Websites und Anwendungen hinzufügen, denen Sie auch wirklich vertrauen. Diese werden dann von den folgenden Engines vom Scan ausgeschlossen: Malware, Phishing und Betrug.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

32.5. Ich kann keine Verbindung zum Internet herstellen

Nach der Installation von Bitdefender werden Sie unter Umständen bemerken, dass ein Programm oder ein Browser keine Verbindung mehr zum Internet herstellen oder auf Netzwerkdienste zugreifen kann.

In diesem Fall ist es die beste Lösung, Bitdefender so zu konfigurieren, dass Verbindungen von und zu der jeweiligen Software-Anwendung automatisch zugelassen werden:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Firewall**.
4. Wählen Sie im Fenster **Firewall** den Reiter **Regeln** aus.
5. Klicken Sie auf die Schaltfläche **Regel hinzufügen**, um eine Anwendungsregel hinzuzufügen.
6. Es öffnet sich ein neues Fenster, in dem Sie die Details hinzufügen können. Stellen Sie sicher, dass Sie alle verfügbaren Netzwerktypen auswählen und klicken Sie im Bereich **Berechtigung** auf **Zulassen**.

Schließen Sie Bitdefender, öffnen Sie die Software-Anwendung und versuchen Sie erneut, eine Verbindung mit dem Internet aufzubauen.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

32.6. Ich kann auf ein Gerät in meinem Netzwerk nicht zugreifen

Abhängig von dem Netzwerk mit dem Sie verbunden sind, könnte die Bitdefender-Firewall die Verbindung zwischen Ihrem System und einem anderen Gerät (zum Beispiel einem anderen Computer oder Drucker) blockieren. Dadurch sind Sie vielleicht nicht mehr in der Lage, Dateien auszutauschen oder zu drucken.

In diesem Fall ist es die beste Lösung, Bitdefender so zu konfigurieren, dass Verbindungen von und zu dem jeweiligen Gerät automatisch zugelassen werden. Sie können für jede Netzwerkverbindung eine eigene vertrauenswürdige Zone konfigurieren.

Ein vertrauenswürdige Zone ist ein Gerät, dem Sie uneingeschränkt vertrauen. Jeglicher Datenverkehr zwischen Ihrem Computer und dem vertrauenswürdigen Gerät wird zugelassen. Um Ressourcen mit bestimmten Geräten wie anderen Computern oder Druckern zu teilen, fügen Sie diese als vertrauenswürdige Zonen hinzu.

Um Ihren Netzwerkadaptern eine vertrauenswürdige Zone hinzuzufügen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Firewall**.
4. Wählen Sie im Fenster **Firewall** den Reiter **Regeln** aus.
5. Klicken Sie auf die Schaltfläche **Regel hinzufügen**, um eine Zone hinzuzufügen. Ein neues Fenster mit den IP-Adressen der mit dem Netzwerk verbundenen Geräte wird angezeigt.
6. Wählen Sie die IP-Adresse des Computers oder den Drucker, den Sie hinzufügen wollen, oder geben Sie eine Adresse oder einen Adressbereich in das entsprechende Textfeld ein.
7. Wählen Sie im Feld **Berechtigung Zulassen** aus und klicken Sie dann auf **OK**.

Wenn eine Verbindung mit dem Gerät immer noch nicht möglich ist, wird das Problem vielleicht nicht durch Bitdefender hervorgerufen.

Überprüfen Sie andere mögliche Ursachen, wie z.B:

- Die Firewall auf dem anderen Computer könnte die Nutzung des gemeinsamen Druckers oder der Datei blockieren.
  - Wenn die Windows Firewall genutzt wird, kann diese wie folgt zum Zulassen von Datei- und Druckerfreigabe konfiguriert werden:
    - In **Windows XP**:
      1. Klicken Sie auf **Start**, öffnen Sie die **Systemsteuerung** und wählen Sie **Sicherheitscenter**.
      2. Öffnen Sie das Einstellungsfenster für die Windows Firewall und klicken Sie auf den Reiter **Ausnahmen**.
      3. Wählen Sie die Option **Datei- und Druckerfreigabe**.
    - In **Windows Vista und Windows 7**:

1. Klicken Sie auf **Start**, öffnen Sie die **Systemsteuerung** und wählen Sie **System und Sicherheit**.
2. Öffnen Sie die **Windows-Firewall** und wählen Sie **Programm durch die Windows-Firewall kommunizieren lassen**.
3. Wählen Sie die Option **Datei- und Druckerfreigabe**.

- In **Windows 8**:

1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
2. Klicken Sie auf **System und Sicherheit**, öffnen Sie die **Windows-Firewall** und wählen Sie **Apps über die Windows-Firewall kommunizieren lassen**.
3. Wählen Sie die Option **Datei- und Druckerfreigabe** und klicken Sie **OK**.

- Wenn eine andere Firewall verwendet wird, greifen Sie bitte auf die entsprechende Dokumentation oder Hilfedatei zurück.

- Allgemeine Umstände, die eine Benutzung des oder Verbindung mit dem freigegebenen Drucker verhindern könnten:
  - Möglicherweise müssen Sie sich als Windows-Administrator anmelden, um auf den freigegebenen Drucker zugreifen zu können.
  - Für den gemeinsam genutzten Drucker werden Rechte vergeben, so dass dieser nur bestimmten Computern und Benutzern den Zugriff erlaubt. Falls Sie Ihren Drucker zur gemeinsamen Nutzung freigegeben haben, überprüfen Sie die Rechte, die für den Drucker vergeben wurden, um festzustellen, ob der Nutzer des anderen Computers Zugriffsrechte erhalten hat. Wenn Sie versuchen, eine Verbindung zu einem freigegebenen Drucker aufzubauen, sollten Sie mit Benutzer auf dem anderen Computer abklären, ob Sie die benötigten Rechte haben.
  - Der Drucker, der mit Ihren Computer oder dem anderen Computer verbunden ist, ist nicht freigegeben.
  - Der freigegebene Drucker wurde dem Computer nicht hinzugefügt.

Beachten Sie

Um mehr darüber zu erfahren, wie Sie die Druckerfreigabe verwalten können (Drucker freigeben, Rechte vergeben oder entziehen, Verbindungen mit

einen freigegebenen Drucker herstellen), klicken sie im Windows-Startmenü auf **Hilfe und Support**).

- Der Zugriff auf einen Netzwerk-Drucker könnte auf bestimmte Computer oder Nutzer beschränkt sein. Fragen Sie Ihren Netzwerk-Administrator, ob Sie die notwendigen Rechte besitzen, um auf diesen Drucker zuzugreifen.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

32.7. Meine Internetverbindung ist langsam

Diese Situation könnte nach der Installation von Bitdefender eintreten. Das Problem könnte aufgrund von Konfigurationsfehlern der Bitdefender-Firewall auftreten.

Zur Behebung dieses Problems gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Klicken Sie auf das Modul **Firewall**.
4. Klicken Sie im Fenster **Firewall** auf den Schalter, um die **Firewall** zu deaktivieren.
5. Überprüfen Sie, ob Sie nach der Deaktivierung der Bitdefender-Firewall eine Verbesserung der Internet-Verbindung feststellen können.
   - Wenn die Internetverbindung immer noch langsam ist, wird das Problem vielleicht nicht durch Bitdefender hervorgerufen. Sie sollten Ihren Internet-Provider kontaktieren, um abzuklären, dass es von seiner Seite aus keine Verbindungsprobleme gibt.

     Wenn Sie von Ihrem Internet-Anbieter die Bestätigung erhalten, dass es auf Anbieterseite keine Probleme gibt und das Problem besteht weiterhin, kontaktieren Sie Bitdefender wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.
   - Falls Sie nach der Deaktivierung der Bitdefender-Firewall eine Verbesserung der Internet-Verbindung feststellen können, gehen Sie folgendermaßen vor:
     a. Öffnen Sie das Bitdefender-Fenster.
     b. Öffnen die den Bereich **Schutz**.

c. Klicken Sie auf das Modul **Firewall**.

d. Wählen Sie im Fenster **Firewall** den Reiter **Einstellungen** aus.

e. Gehen Sie in den Bereich **Gemeinsame Nutzung der Internetverbindung blockieren** und klicken Sie auf den Schalter, um dies zu aktivieren.

f. Gehen Sie in den Bereich **Gemeinsame Nutzung der Internetverbindung blockieren** und klicken Sie auf den Schalter, um dies zu deaktivieren.

g. Rufen Sie den Reiter **Adapter** auf und wählen Sie Ihre Internet-Verbindung aus.

h. Wählen Sie in der Spalte **Netzwerktyp** den Punkt **Heim/Büro** aus.

i. Wählen Sie in der Spalte **Tarnkappe** den Punkt **Remote** aus. Setzen Sie die Spalte **Generisch** auf **An**.

j. Schließen Sie Bitdefender, starten Sie das System neu und überprüfen Sie die Internet-Verbindungsgeschwindigkeit.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

32.8. Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann

Falls Sie über eine langsame Internet-Verbindung (wie z. B. ein Modem) verfügen, können während des Updates Fehler auftreten.

Um Ihr System hinsichtlich Bitdefender-Malware-Signaturen auf dem neuesten Stand zu halten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
3. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Update** aus.
4. Wählen Sie neben **Update-Verarbeitungsregeln** den Eintrag **Vor dem Download nachfragen** aus dem Menü aus.
5. Kehren Sie zum Hauptfenster zurück und klicken Sie rechts im Fenster auf die Schaltfläche **Update**.

6. Wählen Sie nur **Signatur-Updates** und klicken Sie dann auf **OK**.
7. Bitdefender wird nur die Malware-Signatur-Updates herunterladen und installieren.

32.9. Mein Computer ist nicht mit dem Internet verbunden. Wie kann ich Bitdefender aktualisieren?

Wenn Ihr Computer über keine Internet-Verbindung verfügt, müssen Sie die Updates manuell auf einen Computer mit Internet-Zugang herunterladen und dann über einen Wechseldatenträger wie beispielsweise einen USB-Speicherstick auf Ihren Rechner transferieren.

Folgen Sie diesen Schritten:

1. Öffnen Sie auf einem Computer mit Internet-Zugang einen Web-Browser und gehen Sie auf:

   http://www.bitdefender.de/site/view/Desktop-Products-Updates.html
2. Klicken Sie in der Spalte **Manuelles Update** auf den entsprechenden Link für Ihr Produkt und Ihre Systemarchitektur. Wenn Sie nicht wissen, ob auf Ihrem Computer eine 32-Bit- oder 64-Bit-Version von Windows ausgeführt wird, lesen Sie bitte *„Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert?“* (S. 85).
3. Speichern Sie die Datei namens weekly.exe im System.
4. Übertragen Sie die heruntergeladene Datei zunächst auf einen Wechseldatenträger wie beispielsweise einen USB-Speicherstick und dann auf Ihren Computer.
5. Doppelklicken Sie auf die Datei und folgen Sie den Anweisungen des Assistenten.

32.10. Bitdefender-Dienste antworten nicht

Dieser Artikel hilft Ihnen bei der Lösung des Problems **Bitdefender-Dienste antworten nicht**. Sie könnten folgende Fehlermeldung erhalten:

- Das Bitdefender-Symbol im der Task-Leiste ist grau hinterlegt und Sie erhalten eine Meldung, dass die Bitdefender-Dienste nicht reagieren.
- Das Bitdefender-Fenster zeigt an, dass die Bitdefender-Dienste nicht antworten.

Der Fehler kann durch einen der folgenden Umstände verursacht werden:

- Temporäre Kommunikationsstörungen zwischen den Bitdefender-Diensten.
- Einige der Bitdefender-Dienste wurden angehalten.
- Andere Sicherheitslösungen laufen gleichzeitig mit Bitdefender auf Ihrem Rechner.

Um diesen Fehler zu beheben, versuchen Sie folgenden Lösungen:

1. Warten Sie einen Moment und beobachten Sie, ob sich etwas ändert. Der Fehler könnte vorübergehend sein.
2. Starten Sie den Rechner neu und warten Sie einige Momente, bis Bitdefender geladen ist. Öffnen Sie Bitdefender und überprüffen Sie ob das Problem immernoch besteht. Durch einen Neustart des Computers wird das Problem normalerweise gelöst.
3. Überprüfen Sie, ob Sie irgendeine andere Sicherheitslösung installiert haben, weil diese den Normalbetrieb von Bitdefender stören könnte. Wenn dies der Fall ist, empfehlen wir Ihnen alle anderen Sicherheitslösungen zu entfernen und Bitdefender wieder neu zu installieren.

   Für weitere Informationen lesen Sie bitte *„Wie entferne ich andere Sicherheitslösungen?“* (S. 86).

Sollte der Fehler weiterhin auftreten, wenden Sie sich bitte an unsere Support-Mitarbeiter, wie in Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

32.11. Der Spam-Schutz-Filter funktioniert nicht richtig

Dieser Artikel hilft Ihnen, folgende Probleme mit dem Bitdefender Antispam-Filter lösen:

- Eine Anzahl von seriösen E-Mails werden markiert als [spam].
- Viele Spams werden entsprechend nicht durch den Antispam Filter markiert.
- Der Antispam-Filter entdeckt keine Spamnachrichten.

32.11.1. Legitime Nachrichten werden als [spam] markiert

Seriöse Nachrichten werden als [spam] markiert, einfach deshalb weil sie für den Bitdefender Antispam-Filter wie solche aussehen. Im Normalfall

können Sie dieses Problem lösen indem Sie den Antispam Filter angemessen konfigurieren.

Bitdefender fügt die Empfänger Ihrer Mails automatisch der Freundeliste hinzu. Die E-Mails, die von Kontakten in der Freunde Liste empfangen werden, werden als seriös angesehen. Sie werden nicht vom Spam-Filter geprüft und deshalb auch nie als [spam] markiert.

Die automatische Konfiguration der Freundesliste verhindert nicht die entdeckte Störungen, die in dieser Situationen auftreten können:

- Sie empfangen viele angeforderte Werb-E-Mails resultierend aus der Anmeldung auf verschiedene Webseiten. In diesem Fall ist die Lösung, die E-Mail Adressen, von denen Sie solche E-Mails bekommen, auf die Freunde Liste zu setzen.
- Ein erheblicher Teil Ihrer legitimen Email ist von Leuten, die bisher nie E-Mails von Ihnen erhalten haben. bspw. Kunden, potentielle Geschäftspartner und andere. Andere Lösungen sind in diesem Fall erforderlich.

  Wenn Sie einen der Mail-Clients nutzen, in die sich Bitdefender integriert, weisen Sie auf Erkennungsfehler hin.



Beachten Sie

Bitdefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste. Um die komplette Liste der unterstützen E-Mail Clients, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle“* (S. 120).

Kontakte zur Freundesliste hinzufügen

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder ganz leicht zu der Freundesliste hinzufügen. Folgen Sie diesen Schritten:

1. Wählen Sie in Ihrem Mail Client eine Mail eines Senders, den Sie der Freundesliste hinzufügen möchten.
2. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste auf die Schaltfläche **Neuer Freund**.

3. Es kann sein das Sie die Adressen, die zur Freundesliste hinzugefügt wurden, bestätigen müssen. Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **OK**.

Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.

Falls Sie einen anderen Mail Client verwenden, können Sie von der Bitdefender-Oberfläche aus Kontakte der Freundeliste hinzufügen. Folgen Sie diesen Schritten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Wählen Sie im Modul **Spam-Schutz Freunde verwalten** aus.

   Ein Konfigurationsfenster wird sich öffnen.
4. Geben Sie die E-Mail-Adresse ein, von der Sie immer E-Mails empfangen wollen und klicken Sie auf **Hinzufügen**. Sie können beliebig viele E-Mail-Adressen hinzufügen.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Auf Erkennungsfehler hinweisen

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie den Spam-Filter einfach korrigieren (indem Sie angeben, welche E-Mails nicht als [spam] hätten markiert werden sollen). Dadurch wird die Effizienz des Spam-Filters verbessert. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Wählen Sie die Nachricht, die von Bitdefender fälschlicherweise als [spam] markiert wurde, aus.
4. Klicken Sie auf **Neuer Freund** in der Bitdefender-Spam-Schutz-Symbolleiste. Klicken Sie zur Bestätigung **OK**. Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.
5. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die

Schaltfläche **Kein Spam**. Die E-Mail wird in den Posteingangsordner verschoben.

32.11.2. Eine Vielzahl von Spam-Nachrichten wird nicht erkannt

Wenn Sie viele Nachrichten erhalten, die nicht als [spam] markiert sind, konfigurieren Sie den Bitdefender Antispam-Filter, um seine Effektivität zu erhöhen.

Versuchen Sie die folgenden Lösungsansätze:

1. Wenn Sie einen der Mail-Clients nutzen, in die sich Bitdefender integriert, weisen Sie auf unerkannte Spam-Nachrichten hin.



Beachten Sie

Bitdefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste. Um die komplette Liste der unterstützen E-Mail Clients, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle“* (S. 120).

2. Neuen Spammer zur Liste der Spammer hinzufügen. Die E-Mail-Nachrichten, die von den Adressen aus der Spammerliste empfangen werden, werden automatisch markiert als [spam].

Auf unerkannte Spam-Nachrichten hinweisen

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie einfach angeben, welche E-Mails als Spam hätten markiert werden sollen. Dadurch wird die Effizienz des Spam-Filters verbessert. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Begeben Sie sich zum Inbox Ordner.
3. Wählen Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Ist Spam**. Sie werden dann sofort als [spam] markiert und in den Junk-Ordner verschoben.

Neue Spammer zur Liste der Spammer hinzufügen

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder der Spamnachricht ganz leicht zu der Spammerliste hinzufügen. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Markieren Sie die Nachricht die von Bitdefender als [spam] markiert wurde.
4. Klicken Sie in der Bitdefender-Spam-Schutz-Leiste auf **Neuer Spammer**.
5. Es kann sein das Sie die Adresse bestätigen müssen, die in der Spammerliste hinzugefügt wurde. Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **OK**.

Falls Sie einen anderen E-Mail-Client verwenden, können Sie von der Bitdefender-Oberfläche aus manuell Spammer der Liste der Spammer hinzufügen. Dies sollten Sie nur dann tun, wenn Sie bereits mehrere Spam-Nachrichten vom selben Absender erhalten haben. Folgen Sie diesen Schritten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Wählen Sie im Modul **Spam-Schutz Spammer verwalten** aus.

   Ein Konfigurationsfenster wird sich öffnen.
4. Geben Sie die E-Mail-Adresse des Spammers ein und klicken Sie auf **Hinzufügen**. Sie können beliebig viele E-Mail-Adressen hinzufügen.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

32.11.3. Der Spam-Schutz-Filter erkennt keine Spam-Nachrichten

Wenn keine Nachrichten als [spam] markiert werden, könnte es möglicherweise am Bitdefender Antispam Fileter liegen. Vor der Fehlersuche dieses Problems, sollten Sie sicherstellen , dass es nicht durch einen der folgenden Bedingungen verursacht wird:

- Der Spam-Schutz ist unter Umständen deaktiviert. Um den Status Ihres Spam-Schutzes zu überprüfen, öffnen Sie das Bitdefender-Fenster, gehen Sie in den Bereich **Schutz**, klicken Sie auf das Modul **Spam-Schutz** und überprüfen Sie die Stellung des Schalters im Fenster **Einstellungen**.

  Falls der Spam-Schutz deaktiviert ist, so liegt hier die Ursache Ihres Problems. Klicken Sie auf den Schalter, um Ihren Spam-Schutz zu aktivieren.

- Der Bitdefender Antispam-Schutz ist nur für Email Clients verfügbar, die Emails über das POP3-Protokoll zu empfangen. Das bedeutet folgendes:
  - Die Email-Nachrichten, die über web-basierte Email-Dienstleistungen empfangen werden (wie Yahoo, Gmail, Hotmail oder andere) gehen nichtdurch den Bitdefender Spam-Filter.
  - Wenn Ihr Email Client konfiguriert ist, Emails unter Verwendung anderer Protokolle als POP3 zu empfangen (z.B., IMAP4), scannt der Bitdefender Antispam-Filter diese Emails nicht auf Spam-Mails.



Beachten Sie

POP3 ist eines der am meisten benutzten Protokolle für das Downloaden der E-Mail-Nachrichten vom Mail-Server. Falls Sie das Protokoll nicht kennen, das von Ihrem E-Mail Client benutzt wird, um E-Mail Nachrichten herunterzuladen, fragen Sie die Person, die Ihren E-Mail Client konfiguriert hat.

- Bitdefender Internet Security 2015 scannt keine POP3-Übertragungen von Lotus Notes.

Es könnte sein, dass das Problem durch eine Reparatur oder Neuinstallation des Produkts behoben wird. Falls Sie lieber den Bitdefender-Kundendienst kontaktieren möchten, folgen Sie der Beschreibung im Abschnitt *„Hilfe anfordern“* (S. 238).

32.12. Das automatische Einfügen funktioniert bei meiner Geldbörse nicht

Sie haben Ihre Online-Anmeldedaten bereits in Ihrer Bitdefender-Geldbörse gespeichert und das automatische Einfügen funktioniert nicht. Dies geschieht in aller Regel, wenn die Erweiterung für die Bitdefender-Geldbörse in Ihrem Browser nicht installiert wurde.

Um das Problem zu beheben, gehen Sie folgendermaßen vor:

- Im **Internet Explorer:**
  1. Öffnen Sie den Internet Explorer.
  2. Klicken Sie auf Extras.
  3. Klicken Sie auf Add-Ons verwalten.
  4. Klicken Sie auf Symbolleisten und Erweiterungen.
  5. Bewegen Sie den Mauszeiger auf **Bitdefender-Geldbörse** und klicken Sie Aktivieren.
- In **Mozilla Firefox:**
  1. Öffnen Sie Mozilla Firefox.
  2. Klicken Sie auf Extras.
  3. Klicken Sie auf Add-ons.
  4. Klicken Sie auf Erweiterungen.
  5. Bewegen Sie den Mauszeiger auf **Bitdefender-Geldbörse** und klicken Sie Aktivieren.
- In **Google Chrome:**
  1. Öffnen Sie Google Chrome.
  2. Klicken Sie auf das Menü-Symbol.
  3. Klicken Sie auf Einstellungen.
  4. Klicken Sie auf Erweiterungen.
  5. Bewegen Sie den Mauszeiger auf **Bitdefender-Geldbörse** und klicken Sie Aktivieren.



Beachten Sie

Das Add-on wird nach einem Neustart des Browsers aktiviert.

Überprüfen Sie jetzt, ob das automatische Einfügen für Ihre Online-Benutzerkonten funktioniert.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

32.13. Entfernen von Bitdefender ist fehlgeschlagen

Wenn Sie Ihr Bitdefender-Produkt deinstallieren möchten und Sie bemerken, dass der Prozess hängen bleibt oder das System einfriert, klicken Sie auf **Abbrechen**. Sollte dies nicht zum Erfolg führen, starten Sie den Computer neu.

Falls die Deinstallation fehlschlägt, bleiben unter Umständen einige Bitdefender-Registry-Schlüssel und Dateien in Ihrem System. Solche Überbleibsel können eine erneute Installation von Bitdefender verhindern. Ebenso kann die Systemleistung und Stabilität leiden.

Um Bitdefender vollständig von Ihrem System zu entfernen, gehen Sie folgendermaßen vor:

- In **Windows XP**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme hinzufügen/entfernen**.
  2. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Entfernen**.
  3. Klicken Sie im angezeigten Fenster auf **Entfernen**.
  4. Hier sind die folgenden Optionen verfügbar:
     - **Ich möchte es erneut installieren** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird nicht installiert.
     - **Ich möchte es dauerhaft entfernen** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird zum Schutz vor Malware auf Ihrem System installiert.

     Wählen Sie die gewünschte Option und klicken Sie auf **Weiter**.
  5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
- Für **Windows Vista** und **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.
  3. Klicken Sie im angezeigten Fenster auf **Entfernen**.

4. Hier sind die folgenden Optionen verfügbar:
   - **Ich möchte es erneut installieren** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird nicht installiert.
   - **Ich möchte es dauerhaft entfernen** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird zum Schutz vor Malware auf Ihrem System installiert.

   Wählen Sie die gewünschte Option und klicken Sie auf **Weiter**.
5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- In **Windows 8**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.
  4. Klicken Sie im angezeigten Fenster auf **Entfernen**.
  5. Hier sind die folgenden Optionen verfügbar:
     - **Ich möchte es erneut installieren** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird nicht installiert.
     - **Ich möchte es dauerhaft entfernen** - wird Bitdefender vollständig entfernen. Der Bitdefender-60-Sekunden-Viren-Scanner wird zum Schutz vor Malware auf Ihrem System installiert.

     Wählen Sie die gewünschte Option und klicken Sie auf **Weiter**.
  6. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.



Beachten Sie

Der Bitdefender-60-Sekunden-Viren-Scanner ist eine kostenlose Anwendung, die auf In-the-Cloud-Scans setzt, um schädliche Programme und Bedrohungen in weniger als 60 Sekunden zu erkennen.

32.14. Mein System fährt nach der Installation von Bitdefender nicht mehr hoch

Wenn Sie Bitdefender gerade installiert haben und Ihr System nicht mehr im Normalmodus starten können, kann es verschiedene Ursachen für dieses Problem geben.

Höchstwahrscheinlich wird es durch eine vorherige Bitdefender-Installation hervorgerufen, die nicht vollständig entfernt wurde. Eine weitere Möglichkeit ist eine andere Sicherheitslösung, die noch auf dem System installiert ist.

Im Folgenden finden Sie Herangehensweisen für die verschiedenen Situationen:

- **Sie hatten Bitdefender schon einmal im Einsatz und danach nicht vollständig von Ihrem System entfernt.**

  Um dieses Problem zu lösen, gehen Sie folgendermaßen vor:

  1. Starten Sie Ihren Computer im abgesicherten Modus neu. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 89).
  2. Entfernen Sie Bitdefender von Ihrem System:
     - In **Windows XP**:
       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme hinzufügen/entfernen**.
       b. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Entfernen**.
       c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.
       d. Klicken Sie auf **Weiter**.
       e. Heben Sie die Markierung bei **Den Bitdefender-60-Sekunden-Viren-Scanner installieren** auf und klicken Sie auf **Weiter**.
       f. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.
       g. Starten Sie Ihren Computer im Normalmodus neu.
     - Für **Windows Vista** und **Windows 7**:

a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.

b. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.

c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

d. Klicken Sie auf **Weiter**.

e. Heben Sie die Markierung bei **Den Bitdefender-60-Sekunden-Viren-Scanner installieren** auf und klicken Sie auf **Weiter**.

f. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.

g. Starten Sie Ihren Computer im Normalmodus neu.

- In **Windows 8**:

a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

c. Suchen Sie **Bitdefender Internet Security 2015** und wählen Sie **Deinstallieren**.

d. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

e. Klicken Sie auf **Weiter**.

f. Heben Sie die Markierung bei **Den Bitdefender-60-Sekunden-Viren-Scanner installieren** auf und klicken Sie auf **Weiter**.

g. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.

h. Starten Sie Ihren Computer im Normalmodus neu.

3. Installieren Sie Ihr Bitdefender-Produkt erneut.

- **Sie hatten zuvor eine andere Sicherheitslösung im Einsatz und haben diese nicht vollständig entfernt.**

Um dieses Problem zu lösen, gehen Sie folgendermaßen vor:

1. Starten Sie Ihren Computer im abgesicherten Modus neu. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 89).
2. Entfernen Sie die andere Sicherheitslösung von Ihrem System:
   - In **Windows XP**:
     a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme hinzufügen/entfernen**.
     b. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
     c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
     d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
   - Für **Windows Vista** und **Windows 7**:
     a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
     b. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
     c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
     d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
   - In **Windows 8**:
     a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
     b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
     c. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
     d. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.

e. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

Um die andere Software vollständig zu deinstallieren, rufen Sie die Hersteller-Website auf und führen Sie das entsprechende Deinstallations-Tool aus oder wenden Sie sich direkt an den Hersteller, um eine Deinstallationsanleitung zu erhalten.

3. Starten Sie Ihr System im Normalmodus neu und installieren Sie Bitdefender erneut.

Sie haben die oben beschriebenen Schritte bereits durchgeführt und das Problem besteht weiterhin.

Um dieses Problem zu lösen, gehen Sie folgendermaßen vor:

1. Starten Sie Ihren Computer im abgesicherten Modus neu. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 89).
2. Nutzen Sie die Systemwiederherstellung von Windows, um den Computer zu einem früheren Zeitpunkt wiederherzustellen, bevor das Bitdefender-Produkt installiert wurde. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie nutze ich die Systemwiederherstellung unter Windows?“* (S. 87).
3. Starten Sie das System im Normalmodus neu und wenden Sie sich an unsere Support-Mitarbeiter, wie in Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

33. MALWARE VON IHREM SYSTEM ENTFERNEN

Malware kann Ihr System auf vielfältige Art und Weise beeinflussen. Wie Bitdefender auf diese Malware reagiert, hängt von der Art des Malware-Angriffs ab. Da Viren ihr Verhalten ständig ändern, ist es schwierig ein Muster für ihr Verhalten und Aktionen festzulegen.

Es gibt Situationen, in denen Bitdefender eine Malware-Infizierung Ihres Systems nicht automatisch entfernen kann. In solch einem Fall ist Ihre Intervention nötig.

- *„Bitdefender-Rettungsmodus“* (S. 225)
- *„Wie gehe ich vor, wenn Bitdefender einen Virus auf Ihrem Computer findet?“* (S. 228)
- *„Wie entferne ich einen Virus aus einem Archiv?“* (S. 229)
- *„Wie entferne ich einen Virus aus einem E-Mail-Archiv?“* (S. 231)
- *„Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?“* (S. 232)
- *„Wie Sie infizierte Dateien aus dem Ordner "System Volume Information" entfernen können“* (S. 232)
- *„Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?“* (S. 234)
- *„Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?“* (S. 235)
- *„Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?“* (S. 235)
- *„Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?“* (S. 235)

Wenn Sie Ihr Problem hier nicht finden oder wenn die vorgeschlagene Lösung nicht zum Erfolg führt, können Sie den technischen Kundendienst von Bitdefender wie in Kapitel *„Hilfe anfordern“* (S. 238) beschrieben, kontaktieren.

33.1. Bitdefender-Rettungsmodus

Der **Rettungsmodus** ist eine Bitdefender-Funktion, mit der Sie alle bestehenden Festplattenpartitionen unabhängig von Ihrem Betriebssystem scannen und desinfizieren können.

Sobald Bitdefender Internet Security 2015 installiert wurde, kann der Rettungsmodus genutzt werden, selbst wenn Sie Ihr System unter Windows nicht mehr hochfahren können.

Starten Ihres Systems im Rettungsmodus

Es gibt zwei Möglichkeiten, den Rettungsmodus zu starten:

Über das Bitdefender-Fenster

Um den Rettungsmodus direkt aus Bitdefender heraus zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Öffnen die den Bereich **Schutz**.
3. Wählen Sie im Modul **Virenschutz Rettungsmodus** aus.

   Ein Bestätigungsfenster wird angezeigt. Bitte klicken Sie auf **Ja**, um Ihren Computer neu zu starten.
4. Nach dem Neustart des Computers erscheint ein Menü, das Sie dazu auffordert, ein Betriebssystem auszuwählen. Wählen Sie **Bitdefender-Rettungsmodus** aus und drücken Sie die **Eingabetaste**, um den Computer in einer Bitdefender-Umgebung zu starten, in der Sie Ihre Windows-Partition bereinigen können.
5. Wenn Sie dazu aufgefordert werden, drücken Sie die **Enter**-Taste und wählen Sie die Bildschirmauflösung, die am ehesten der von Ihnen sonst verwendeten Auflösung entspricht. Drücken Sie die **Eingabetaste** erneut.

   Der Bitdefender-Rettungsmodus wird innerhalb weniger Momente geladen.

Starten des Computers im Rettungsmodus

Wenn Windows nicht mehr startet, können Sie Ihren Computer direkt im Bitdefender-Rettungsmodus neu starten, indem Sie folgendermaßen vorgehen:



Beachten Sie

Diese Methode ist auf Computern mit Windows XP nicht verfügbar.

1. Starten Sie Ihren Computer bzw. führen Sie einen Neustart durch und fangen Sie an, die **Leertaste** zu drücken, bevor das Windows-Logo erscheint.

2. Ein Menü erscheint und fordert Sie auf, ein Betriebssystem für den Start auszuwählen. Drücken Sie auf die **Tabulatortaste**, um in den Tools-Bereich zu wechseln. Wählen Sie **Bitdefender Rescue Image** und drücken Sie die **Eingabetaste**, um den Computer in einer Bitdefender-Umgebung zu starten, von der aus Sie Ihre Windows-Partition bereinigen können.
3. Wenn Sie dazu aufgefordert werden, drücken Sie die **Enter**-Taste und wählen Sie die Bildschirmauflösung, die am ehesten der von Ihnen sonst verwendeten Auflösung entspricht. Drücken Sie die **Eingabetaste** erneut.

   Der Bitdefender-Rettungsmodus wird innerhalb weniger Momente geladen.

Scannen Ihres Systems im Rettungsmodus

Um Ihr System im Rettungsmodus zu scannen, gehen Sie folgendermaßen vor:

1. Starten Sie den Rettungsmodus, wie in Kapitel „Starten Ihres Systems im Rettungsmodus“ (S. 226) beschrieben.
2. Das Bitdefender-Logo wird angezeigt und der Kopiervorgang für die Virenschutz-Engines beginnt.
3. Ein Willkommensfenster wird angezeigt. Klicken Sie auf **Fortfahren**.
4. Ein Update der Virensignaturen wird gestartet.
5. Nachdem das Update abgeschlossen ist, erscheint das Fenster für den Bitdefender-Bedarf-Scan.
6. Klicken Sie auf **Jetzt scannen**, wählen Sie in dem jetzt erscheinenden Fenster das Scan-Ziel aus und klicken Sie auf **Öffnen**, um den Scan zu starten.

   Wir empfehlen Ihnen, Ihre gesamte Windows-Partition zu scannen.



Beachten Sie

Wenn Sie den Rettungsmodus nutzen, werden Ihnen die Namen der Partitionen im Linux-Format angezeigt. Die Festplattenpartitionen werden angezeigt als sda1, was wahrscheinlich der Windows-Partition (C:) entspricht, sda2, was (D:) entspricht usw.

7. Warten Sie, bis der Scan abgeschlossen ist. Falls Malware gefunden wurde, folgen Sie den Anweisungen, um die Bedrohung zu entfernen.
8. Um den Rettungsmodus zu beenden, klicken Sie mit der rechten Maustaste auf einen leeren Bereich auf dem Desktop, klicken Sie im Kontextmenü auf **Verlassen** und wählen Sie dann, ob Sie den Computer neu starten oder herunterfahren möchten.

33.2. Wie gehe ich vor, wenn Bitdefender einen Virus auf Ihrem Computer findet?

Es gibt verschiedene Möglichkeiten, Ihnen mitzuteilen, ob sich auf Ihrem Computer Viren befinden:

- Sie haben einen Scan durchgeführt und Bitdefender hat infizierte Einträge gefunden.
- Ein Virenwarnhinweis informiert Sie, dass Bitdefender einen oder mehrere Viren auf Ihrem Computer geblockt hat.

In solchen Situationen sollten Sie Bitdefender aktualisieren, um sicherzustellen, dass Sie über die neuesten Malware-Signaturen verfügen und einen System-Scan durchführen, um das System zu prüfen.

Sobald der System-Scan abgeschlossen ist, wählen Sie die gewünschte Aktion für die infizierten Objekte aus (Desinfizieren, Löschen, In Quarantäne verschieben).



Warnung

Wenn Sie den Verdacht haben, dass die Datei Teil des Windows-Betriebssystems ist oder dass es sich nicht um eine infizierte Datei handelt, folgen Sie NICHT diesen Schritten und kontaktieren Sie so bald wie möglich den Bitdefender-Kundendienst.

Falls die ausgewählte Aktion nicht durchgeführt werden konnte und im Scan-Protokoll ersichtlich ist, dass Ihr PC mit einer Bedrohung infiziert ist, die nicht gelöscht werden kann, müssen Sie die Datei(en) manuell entfernen.

Die erste Methode kann im Normalmodus eingesetzt werden:

1. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Öffnen die den Bereich **Schutz**.

c. Klicken Sie auf das Modul **Virenschutz**.

d. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.

e. Klicken Sie auf den Schalter, um **Zugriff-Scan** zu deaktivieren.

2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 85).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

Sollte die erste Methode, die Infizierung zu entfernen, fehlgeschlagen sein, gehen Sie folgendermaßen vor:

1. Starten Sie Ihren Computer im abgesicherten Modus neu. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 89).
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 85).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Starten Sie Ihren Computer neu und starten Sie den Normalmodus.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

33.3. Wie entferne ich einen Virus aus einem Archiv?

Bei einem Archiv handelt es sich um eine Datei oder eine Dateisammlung, die mit einem speziellen Format komprimiert wurde, um so den benötigten Festplattenplatz zu reduzieren.

Einige dieser Formate sind offene Formate und bieten Bitdefender die Möglichkeit, diese zu scannen und die entsprechenden Aktionen durchzuführen, um sie zu entfernen.

Andere Archivformate sind teilweise oder komplett geschlossen und Bitdefender kann nur das Vorhandensein von Viren innerhalb dieser Archive feststellen, nicht jedoch andere Aktionen ausführen.

Wenn Bitdefender Sie darüber informiert, dass ein Virus innerhalb eines Archivs gefunden wurde und keine Aktion verfügbar ist, bedeutet dies, dass der Virus aufgrund möglicher Restriktionen der Zugriffseinstellungen des Archivs nicht entfernt werden kann.

So können Sie einen in einem Archiv gespeicherten Virus entfernen.

1. Führen Sie einen System-Scan durch, um das Archiv zu finden, in dem sich der Virus befindet.
2. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Öffnen die den Bereich **Schutz**.
   c. Klicken Sie auf das Modul **Virenschutz**.
   d. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.
   e. Klicken Sie auf den Schalter, um **Zugriff-Scan** zu deaktivieren.
3. Gehen Sie zum Speicherort des Archivs und dekomprimieren Sie es mit einem Archivierungsprogramm wie beispielsweise WinZip.
4. Identifizieren Sie die infizierte Datei und löschen Sie sie.
5. Löschen Sie das Originalarchiv, um sicherzugehen, dass die Infizierung vollständig entfernt ist.
6. Komprimieren Sie die Dateien erneut in einem neuen Verzeichnis und verwenden Sie dafür ein Komprimierprogramm wie WinZip.
7. Aktivieren Sie den Bitdefender-Echtzeit-Virenschutz und führen Sie einen Vollsystem-Scan durch, um so sicherzustellen, dass Ihr System nicht anderweitig infiziert ist.



Beachten Sie

Es ist wichtig zu beachten, dass ein in einem Archiv gespeicherter Virus für Ihr System keine unmittelbare Bedrohung darstellt, da der Virus dekomprimiert und ausgeführt werden muss, bevor er Ihr System infizieren kann.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

33.4. Wie entferne ich einen Virus aus einem E-Mail-Archiv?

Bitdefender kann auch Viren in E-Mail-Datenbanken und in auf Festplatten gespeicherten E-Mail-Archiven aufspüren.

Manchmal ist es notwendig, die infizierte Nachricht über die im Scan-Bericht zur Verfügung gestellten Informationen zu identifizieren und sie dann manuell zu löschen.

So können Sie in einem E-Mail-Archiv gespeicherte Viren entfernen:

1. Scannen Sie die E-Mail-Datenbank mit Bitdefender.
2. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Öffnen die den Bereich **Schutz**.
   c. Klicken Sie auf das Modul **Virenschutz**.
   d. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.
   e. Klicken Sie auf den Schalter, um **Zugriff-Scan** zu deaktivieren.
3. Öffnen Sie den Scan-Bericht und nutzen Sie die Identifikationsinformation (Betreff, Von, An) der infizierten Nachricht, um den dazugehörigen E-Mail-Client zu finden.
4. Löschen Sie die infizierte Nachricht. Die meisten E-Mail-Clients verschieben gelöschte Nachrichten in ein Wiederherstellungsordner, von dem aus sie wiederhergestellt werden können. Sie sollten sicherstellen, dass die Nachricht auch aus diesem Recovery-Verzeichnis gelöscht ist.
5. Komprimieren Sie das Verzeichnis, in dem die infizierte Nachricht gespeichert wird.
   - In Outlook Express: Klicken Sie im Dateimenü auf "Verzeichnis", dann auf "Alle Verzeichnisse komprimieren".
   - In Microsoft Outlook 2007: Klicken Sie im Dateimenü auf "Datendateiverwaltung". Wählen Sie das persönliche Verzeichnis (.pst), das Sie komprimieren möchten und klicken Sie auf "Einstellungen". Klicken Sie auf Jetzt komprimieren.
   - In Microsoft Outlook 2010 / 2013: Klicken Sie im Dateimenü auf Info und dann Kontoeinstellungen (Konten hinzufügen oder entfernen bzw.

vorhandene Verbindungseinstellungen ändern). Klicken Sie danach auf Datendatei, markieren Sie die persönlichen Ordner-Dateien (.pst), die Sie komprimieren wollen, und klicken Sie auf Einstellungen. Klicken Sie auf Jetzt komprimieren.

6. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

33.5. Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?

Möglicherweise halten Sie eine Datei auf Ihrem System für gefährlich, obwohl Ihr Bitdefender-Produkt keine Gefahr erkannt hat.

Um sicherzustellen, dass Ihr System geschützt ist, gehen Sie folgendermaßen vor:

1. Führen Sie einen **System-Scan** mit Bitdefender durch. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie scanne ich mein System?“* (S. 63).
2. Wenn der Scan ein sauberes Ergebnis liefert, Sie aber weiterhin Zweifel an der Sicherheit der Datei hegen und ganz sicher gehen möchten, wenden Sie sich bitte an unsere Support-Mitarbeiter, damit wir Ihnen helfen können.

   Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Hilfe anfordern“* (S. 238).

33.6. Wie Sie infizierte Dateien aus dem Ordner "System Volume Information" entfernen können

Das Verzeichnis "System Volume Information" ist ein Bereich auf Ihrer Festplatte, der vom Betriebssystem erstellt und von Windows zum Speichern von kritischen Informationen genutzt wird, die in Zusammenhang mit der Systemkonfiguration stehen.

Die Bitdefender-Engine kann infizierte Dateien, die im Verzeichnis "System Volume Information" gespeichert wurden, aufspüren. Da es sich hierbei aber um einen geschützten Bereich handelt, kann die infizierte Datei unter Umständen nicht entfernt werden.

Die in den Systemwiederherstellungsverzeichnissen gefundenen infizierten Dateien werden im Scan-Protokoll wie folgt angezeigt:

?:\System Volume Information_restore{B36120B2-BA0A-4E5D-...

Um infizierte Datei(en) sofort und vollständig aus der Datenspeicherung zu entfernen, deaktivieren und reaktivieren Sie die Funktion "Systemwiederherstellung".

Wenn die Systemwiederherstellung deaktiviert ist, werden alle Wiederherstellungspunkte entfernt.

Wenn die Systemwiederherstellung erneut aktiviert wird, werden neue Wiederherstellungspunkte entsprechend dem Zeitplan und den Ereignissen erstellt.

Um die Systemwiederherstellung zu deaktivieren, gehen Sie folgendermaßen vor:

- **Für Windows XP:**
  1. Folgen Sie diesem Pfad: **Start** → **Alle Programme** → **Zubehör** → **System Tool** → **Systemwiederherstellung**
  2. Klicken Sie in der linken Bildschirmseite auf **Einstellungen Systemwiederherstellung**.
  3. Wählen Sie **Systemwiederherstellung ausschalten** für alle Laufwerke und klicken dann auf **Anwenden**.
  4. Wenn Sie einen Warnhinweis erhalten, dass alle existierenden Wiederherstellungspunkte gelöscht werden, klicken Sie zum Fortfahren auf **Ja**.
  5. Um die Systemwiederherstellung einzuschalten, deaktivieren Sie das Kästchen der Option **Systemwiederherstellung ausschalten** für alle Laufwerke und klicken dann auf **Anwenden**.
- **Für Windows Vista:**
  1. Folgen Sie diesem Pfad: **Start** → **Systemsteuerung** → **System und Wartung** → **System**
  2. Klicken Sie im linken Feld auf **Systemschutz**.

     Wenn Sie zur Eingabe eines Administratorpassworts oder einer Bestätigung aufgefordert werden, geben Sie das Passwort oder die gewünschte Bestätigung ein.

3. Um die Funktion "Systemwiederherstellung" auszuschalten, deaktivieren Sie die entsprechenden Kästchen für jedes Laufwerk und klicken Sie auf **OK**.
4. Um die Systemwiederherstellung zu aktivieren, klicken Sie für jedes Laufwerk die entsprechenden Kästchen an und klicken Sie auf **OK**.

- **Für Windows 7:**
  1. Klicken Sie auf **Start**, rechtsklicken Sie auf **Computer** und danach auf **Eigenschaften**.
  2. Klicken Sie im linken Feld auf den Link **Systemschutz**.
  3. Wählen Sie im Optionenfenster die Option **Systemschutz**, markieren Sie jeden Laufwerksbuchstaben und klicken dann auf **Konfigurieren**.
  4. Wählen Sie **Systemschutz ausschalten** und klicken Sie auf **Anwenden**.
  5. Klicken Sie auf **Löschen**, dann auf **Fortfahren**, wenn Sie dazu aufgefordert werden, und dann auf **Ok**.
- **Für Windows 8:**
  1. Finden Sie auf der Windows-Startseite den **Computer** (z.B. durch die Eingabe von "Computer" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie im linken Feld auf den Link **Systemschutz**.
  3. Wählen Sie im Optionenfenster die Option **Systemschutz**, markieren Sie jeden Laufwerksbuchstaben und klicken dann auf **Konfigurieren**.
  4. Wählen Sie **Systemschutz ausschalten** und klicken Sie auf **Anwenden**.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 238) beschrieben.

33.7. Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?

Dies ist nur eine Benachrichtigung, dass die von Bitdefender gefundenen Dateien entweder passwortgeschützt oder anderweitig verschlüsselt sind.

Am häufigsten sind passwortgeschützte Objekte:

- Dateien, die zu einer anderen Sicherheitslösung gehören.
- Dateien, die zum Betriebssystem gehören.

Um die Inhalte tatsächlich zu scannen, müssen diese Dateien entweder extrahiert oder anderweitig entschlüsselt werden.

Sollten diese Inhalte extrahiert werden, wird der Echtzeit-Scanner von Bitdefender diese automatisch scannen, um so den Schutz Ihres Computers zu gewährleisten. Wenn Sie diese Dateien mit Bitdefender scannen möchten, müssen Sie den Produkthersteller kontaktieren, um nähere Details zu diesen Dateien zu erhalten.

Unsere Empfehlung ist, diese Dateien zu ignorieren, da Sie für Ihr System keine Bedrohung darstellen.

33.8. Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?

Alle Dateien, die im Scan-Protokoll als "Übersprungen" ausgewiesen werden, sind sauber.

Für eine bessere Leistung scannt Bitdefender keine Dateien, die seit dem letzten Scan nicht verändert wurden.

33.9. Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?

Die zu stark komprimierten Objekte sind Elemente, die durch die Scan-Engine nicht extrahiert werden konnten oder Elemente, für die eine Entschlüsselung zu viel Zeit in Anspruch genommen hätte und die dadurch das System instabil machen würden.

Überkomprimiert bedeutet, dass Bitdefender das Scannen von Archiven übersprungen hat, da das Entpacken dieser zu viele Systemressourcen in Anspruch genommen hätte. Der Inhalt wird, wenn nötig, in Echtzeit gescannt.

33.10. Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?

Wird eine infizierte Datei gefunden, versucht Bitdefender automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

Dies geschieht normalerweise bei Installationsdateien, die von nicht vertrauenswürdigen Seiten heruntergeladen werden. Wenn Sie auf ein solches Problem stoßen, laden Sie die Installationsdatei von der Website des Herstellers oder einer anderen vertrauenswürdigen Website herunter.

KONTAKTIEREN SIE UNS

34. HILFE ANFORDERN

Bitdefender bietet seinen Kunden konkurrenzlos schnellen und kompetenten Support. Sollten sich Probleme ergeben oder Sie eine Frage zu Ihrem Bitdefender-Produkt haben, so stehen Ihnen verschiedene Online-Quellen zur Verfügung, wo Sie Lösungen und Antworten finden. Sie können sich auch jederzeit an den Bitdefender-Kundendienst wenden. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.

Im Abschnitt *„Verbreitete Probleme beheben“* (S. 199) finden Sie alle wichtigen Informationen zu den häufigsten Problemen, die bei der Verwendung dieses Produkts auftreten können.

Wenn Sie in den vorhandenen Quellen keine Antwort auf Ihre Frage finden, können Sie uns direkt kontaktieren:

- „Kontaktieren Sie uns direkt aus Ihrem Bitdefender-Produkt heraus“ (S. 238)
- „Kontaktieren Sie uns über unser Online-Support-Center“ (S. 239)



Wichtig

Um den Bitdefender-Kundendienst kontaktieren zu können, müssen Sie Ihr Bitdefender-Produkt registrieren. Für weitere Informationen lesen Sie bitte *„Bitdefender registrieren“* (S. 40).

Kontaktieren Sie uns direkt aus Ihrem Bitdefender-Produkt heraus

Wenn Sie über eine aktive Internet-Verbindung verfügen, können Sie Bitdefender direkt aus der Benutzeroberfläche heraus kontaktieren, um Hilfe zu erhalten.

Folgen Sie diesen Schritten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie oben im Fenster auf das -Symbol und wählen Sie **Hilfe & Support** aus dem Menü aus.
3. Sie haben die folgenden Möglichkeiten:
   - **Produktdokumentation**

Hier können Sie unsere Datenbank nach den gewünschten Informationen durchsuchen.

- **Support kontaktieren**

  Sie können über die Schaltfläche **Kundendienst kontaktieren** das Bitdefender-Support-Tool aufrufen und den Kundendienst kontaktieren. Über die Schaltfläche **Weiter** können Sie im Assistenten blättern. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

  a. Markieren Sie das Zustimmungskästchen und klicken Sie auf **Weiter**.

  b. Geben Sie in das Formular die nötigen Daten ein:

     i. Geben Sie Ihre E-Mail-Adresse ein.

     ii. Geben Sie Ihren vollen Namen ein.

     iii. Beschreiben Sie im Textfeld das Problem, das aufgetreten ist.

     iv. Nutzen Sie die Option **Versuchen Sie, das Problem vor der Übertragung zu reproduzieren**, falls Probleme mit dem Produkt auftreten. Fahren Sie mit den erforderlichen Schritten fort.

  c. Bitte warten Sie einige Minuten, während Bitdefender die produkt-relevanten Informationen einholt. Diese Informationen helfen unseren Mitarbeitern, eine Lösung für Ihr Problem zu finden.

  d. Klicken Sie auf **Beenden**, um die Information an den Bitdefender-Kundendienst zu senden. Sie werden möglichst bald kontaktiert.

Kontaktieren Sie uns über unser Online-Support-Center

Wenn Sie über das Bitdefender-Produkt nicht auf die notwendigen Informationen zugreifen können, wenden Sie sich bitte an unser Online-Support-Center.

1. Gehen Sie zu http://www.bitdefender.de/support/consumer.html.

   Im Bitdefender-Support-Center finden Sie eine Vielzahl von Beiträgen, die Lösungen zu Problemen im Zusammenhang mit Bitdefender bereithalten.

2. Nutzen Sie die Suchleiste oben im Fenster, um Artikel zu finden, die eine Lösung für Ihr Problem enthalten könnten. Geben Sie dazu einen Begriff in die Suchleiste ein und klicken Sie auf **Suchen**.

3. Lesen Sie die relevanten Artikel oder Dokumente und probieren Sie die vorgeschlagenen Lösungen aus.
4. Wenn die dort vorgeschlagene Lösung das Problem nicht behebt, gehen Sie zu

   http://www.bitdefender.de/support/contact-us.htmlund kontaktieren Sie unseren Kundendienst.

35. ONLINE-RESSOURCEN

Für die Lösung Ihres Problems und Fragen im Zusammenhang mit Bitdefender stehen Ihnen verschiedene Online-Ressourcen zur Verfügung.

- Bitdefender-Support-Center:

  http://www.bitdefender.de/support/consumer.html
- Bitdefender Support-Forum:

  http://forum.bitdefender.com
- Das Computer-Sicherheitsportal HOTforSecurity:

  http://www.hotforsecurity.com

Zudem können Sie auch Ihre favorisierte Suchmaschine nutzen, um mehr zu erfahren über Computersicherheit, die Bitdefender-Produkte und das Unternehmen.

35.1. Bitdefender-Support-Center

Das Bitdefender-Support-Center ist eine Online-Sammlung von Informationen zu Ihren Bitdefender-Produkten. Hier sind in einem leicht zugänglichen Format Berichte zu den Ergebnissen des fortlaufenden technischen Supports sowie der Bugfix-Aktivitäten der Bitdefender-Support- und Entwicklungsteams gespeichert. Hinzu kommen Artikel zur Virenvorbeugung, detaillierte Erklärungen zur Verwaltung von Bitdefender-Lösungen und vieles mehr.

Das Bitdefender-Support-Center ist öffentlich zugänglich und frei durchsuchbar. Die darin enthaltenen Informationen sind äußerst umfangreich und stellen eine weitere Methode dar, mit der Bitdefender-Kunden mit dem notwendigen technischen Wissen versorgt werden. Alle berechtigen Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender-Support-Center wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Das Bitdefender-Support-Center steht Ihnen jederzeit unter der folgenden Adresse zur Verfügung:

http://www.bitdefender.de/support/consumer.html.

35.2. Bitdefender Support-Forum

Das Bitdefender Support-Forum bietet Bitdefender-Anwendern eine Möglichkeit, Hilfe zu erhalten oder anderen Hilfestellung zu geben.

Falls Ihr Bitdefender-Produkt nicht richtig funktioniert, bestimmte Viren nicht von Ihrem Computer entfernen kann oder wenn Sie Fragen über die Funktionsweise haben, stellen Sie Ihr Problem oder Frage in das Forum ein.

Support-Techniker von Bitdefender überwachen neue Einträge in das Forum, um Ihnen helfen zu können. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen Bitdefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie bitte im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das Bitdefender Support-Forum finden Sie unter http://forum.bitdefender.com. Es steht in 5 verschiedenen Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch. Für den Zugriff auf den Bereich Konsumgüter klicken Sie bitte auf **Schutz für Privatanwender**.

35.3. Das Portal HOTforSecurity

HOTforSecurity bietet umfangreiche Informationen rund um das Thema Computer-Sicherheit. Hier erfahren Sie mehr über die verschiedenen Bedrohungen, denen Ihr Computer während einer bestehenden Internetverbindung ausgesetzt ist (Malware, Phishing, Spams, Cyber-Kriminelle).

Ständig werden neue Artikel zu den neuesten Threats, aktuellen Sicherheitstrends und anderen Informationen zur Computersicherheits-Branche eingestellt, damit Sie up-to-date bleiben.

Die Adresse von HOTforSecurity ist http://www.hotforsecurity.com.

36. KONTAKTINFORMATIONEN

Effiziente Kommunikation ist der Schlüssel zu einem erfolgreichen Unternehmen. Seit mehr als 10 Jahren überbietet BITDEFENDER konstant die bereits hochgesteckten Erwartungen seiner Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

36.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de
Support-Center:http://www.bitdefender.de/support/consumer.html
Dokumentation: documentation@bitdefender.com
Händler vor Ort:http://www.bitdefender.de/partners
Partnerprogramm: partners@bitdefender.com
Medienkontakt: pr@bitdefender.com
Karriere: jobs@bitdefender.com
Viruseinsendungen: virus_submission@bitdefender.com
Spam-Einsendungen: spam_submission@bitdefender.com
Missbrauch melden: abuse@bitdefender.com
Website:http://www.bitdefender.de

36.2. Lokale Vertriebspartner

Bitdefender-Händler stehen für vertriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung.

So finden Sie einen Bitdefender-Händler in Ihrem Land:

1. Gehen Sie zu http://www.bitdefender.de/partners/#Partner Locator/.
2. Klicken Sie auf den Reiter **Partner-Suche**.
3. Die Kontaktinformationen zum örtlichen Bitdefender Distributor sollten automatisch eingeblendet werden. Sollte dies nicht der Fall sein, so wählen Sie Ihr Land aus, um die Informationen anzuzeigen.
4. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter vertrieb@bitdefender.de kontaktieren. Bitte schreiben Sie uns Ihre Email in englischer Sprache, damit wir Ihnen umgehend helfen können.

36.3. Bitdefender-Niederlassungen

Bitdefender-Niederlassungen stehen Ihnen für betriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Bereichen jederzeit zur Verfügung. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

U.S.A

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefon (Geschäftsstelle&Vertrieb): 1-954-776-6262
Vertrieb: sales@bitdefender.com
Technischer Support: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.com

Großbritannien und Irland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
E-Mail: info@bitdefender.co.uk
Telefon: +44 (0) 8451-305096
Vertrieb: sales@bitdefender.co.uk
Technischer Support: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.co.uk

Deutschland

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Deutschland
Geschäftsstelle: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vertrieb: vertrieb@bitdefender.de
Technischer Support: http://www.bitdefender.de/support/consumer.html
Web: http://www.bitdefender.de

Spain

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Vertrieb: comercial@bitdefender.es
Technischer Support: http://www.bitdefender.es/support/consumer.html
Webseite: http://www.bitdefender.es

Rumänien

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Telefon Vertrieb: +40 21 2063470
Vertrieb E-Mail: sales@bitdefender.ro
Technischer Support: http://www.bitdefender.ro/support/consumer.html
Webseite: http://www.bitdefender.ro

Vereinigte Arabische Emirate

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefon Vertrieb: 00971-4-4588935 / 00971-4-4589186
Vertrieb E-Mail: sales@bitdefender.com
Technischer Support: http://www.bitdefender.com/support/consumer.html
Webseite: http://www.bitdefender.com/world

Glossar

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

AktiveX

ActiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann. Die ActiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden. Mit ActiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen. ActiveX-Steuerelemente werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

Arbeitsspeicher

Interne Speicherbereiche im Rechner. Der Begriff Arbeitsspeicher bezeichnet Datenträger in Form von sehr schnellen Chips. Dies steht im Gegensatz zu Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet. Jeder Rechner hat eine gewisse Menge Arbeitsspeicher. Dieser wird auch Hauptspeicher oder RAM bezeichnet.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Administrator absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon standardmäßig privilegierte Konten eingerichtet, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert. Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Cookie

In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung

anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Anderseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick" verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

Download

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät. Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner. Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

Durchsuchen

Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können. Bekannte Browser sind Microsoft Internet Explorer, Mozilla Firefox und Google Chrome. Dies sind graphische Browser, was bedeutet, dass sie sowohl Grafiken als auch Texte anzeigen können. Weiterhin können die meisten Browser Multimedia-Daten wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

E-Mail

Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

E-Mail Client

Ein E-Mail Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese Scan-Methode benötigt keine spezifischen Virussignaturen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante eines alten Virus getäuscht werden kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Java Applet

Ein Java Programm, das nur auf Webseiten läuft. Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) an, die das Applet einnehmen kann. Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus. Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets z. B. auf dem Client laufen, können diese keine Daten auf der Maschine des Clients lesen oder schreiben. Zusätzlich sind die Applets dahingehend beschränkt, dass sie nur Daten aus der Domain lesen und schreiben können, zu der sie gehören.

Keylogger

Ein Keylogger ist eine Anwendung, die alles aufzeichnet, was Sie tippen.

Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Komprimierte Programme

Eine Datei in einem komprimierten Format. Viele Betriebssysteme und Anwendungen enthalten Befehle, mit denen Dateien komprimiert werden können, sodass diese weniger Speicherplatz benötigen. Zum Beispiel: Angenommen, Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält. Normalerweise belegen diese Leerzeichen dann 10 Bytes an Speicherplatz.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein Sonderzeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden. In diesem Fall sind nur noch zwei Bytes notwendig statt zehn. Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Bitdefender eine Prokolldatei mit den geprüften Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Nicht heuristisch

Diese Scan-Methode beruht auf spezifischen Virussignaturen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einem Scheinvirus getäuscht werden kann und so Fehlalarme verhindert.

Pfad

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Phishing

Beim Phishing wird eine E-Mail mit betrügerischer Absicht an einen Empfänger gesendet, wobei vorgetäuscht wird, die E-Mail stamme von einem bekannten und seriösen Unternehmen. Zweck dieser E-Mail ist es dann, vertrauliche Benutzerdaten wie Passwörter und/oder Kreditkartennummern zu erhalten. Die E-Mail führt den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Photon

Photon ist eine innovative und unaufdringliche Bitdefender-Technologie, die eigens entwickelt wurde, um die Auswirkungen des Virenschutzes auf die Systemleistung zu minimieren. Durch die

Hintergrundüberwachung aller PC-Aktivitäten werden Nutzungsprofile erstellt, mit denen Start- und Scan-Prozesse optimiert werden können.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Rootkit

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Malware zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit Malware stellen sie eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Im Inneren gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Script

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startup Objekt (Autostart-Objekt)

Jede Datei, die sich in diesem Ordner befindet, wird geöffnet, wenn der Rechner gestartet wird. Das können z. B. ein Startbildschirm, eine Sounddatei, die abgespielt wird, wenn der Rechner gestartet wird, ein Erinnerungskalender oder auch Anwendungen sein. Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Task-Leiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Symbole zur Information und zum leichteren Zugriff auf Systemfunktionen wie Drucker, Modems, Lautstärke und anderes. Um auf die Details und Optionen dieser Funktionen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können ebenso schädlich sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update

Eine neue Software- oder Hardwareversion, die eine ältere Version desselben Produkts ersetzt. Die Update-Installationsroutine eines Programms prüft oft, ob eine ältere Versionen auf dem Rechner installiert ist, da sonst kein Update installiert werden kann.

Bitdefender verfügt über ein eigenes Update-Modul, das manuelle oderautomatische Scans nach Updates ermöglicht.

Virus

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Viren können sich auch selbst vervielfältigen. Alle Computerviren wurden von Menschen programmiert. Ein Virus, der sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar ein solch einfacher Virus kann gefährlich sein, da er im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Viren, die sich über Netzwerke selbst weiterversenden und Sicherheitssysteme umgehen.

Virussignatur

Ein binäres Virusmuster, das von einem AntiVirus Programm verwendet wird, um einen Virus zu entdecken und zu entfernen.

Wurm

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.